Avira Premium Security Suite

Manuale utente

Marchio registrato e copyright

Sommario

1 Introduzione 1

2 Simboli ed evidenziazioni 2

3 Informazioni sul prodotto 3

3.1 Prestazioni 3
3.2 Requisiti di sistema 4
3.3 Licenza e aggiornamento 5

4 Installazione e disinstallazione 6

4.1 Installazione........ 6
4.2 Modifiche all'installazione 12
4.3 Moduli di installazione........ 12
4.4 Disinstallazione 13

5 Panoramica 15

5.1 Interfaccia utente e funzionamento 15
5.1.1 Control Center 15
5.1.2 Configurazione........ 18
5.1.3 Icona Tray........ 21
5.2 Come procedere 22
5.2.1 Attiva il prodotto 22
5.2.2 Eseguire gli aggiornamenti automatici 23
5.2.3 Avvio di un aggiornamento manuale 24
5.2.4 Scansione diretta: Eseguire il controllo di virus e malware con un profilo di ricerca 25
5.2.5 Scansione diretta: Ricerca di virus e malware con Drag & Drop........ 27
5.2.6 Scansione diretta: Cerca virus e malware con il menu contestuale 27
5.2.7 Scansione diretta: cerca automaticamente virus e malware 27
5.2.8 Scansione diretta: Effettuare una scansione mirata per rootkit attivi........ 29
5.2.9 Reagire a virus e malware riscontrati........ 29
5.2.10 Quarantena: Trattare file (*.qua) in quarantena 33
5.2.11 Quarantena: Ripristina file in quarantena........ 34
5.2.12 Quarantena: Sposta i file sospetti in quarantena........ 36
5.2.13 Profilo di ricerca: Inserisci o elimina un tipo di file in un profilo di ricerca........ 36
5.2.14 Profilo di ricerca: Creare un collegamento sul desktop per il profilo di ricerca ..37
5.2.15 Eventi: Filtrare eventi 37
5.2.16 MailGuard: Escludere indirizzi email dalla scansione 38
5.2.17 MailGuard: Configurare il modulo AntiSpam........ 38
5.2.18 FireWall: Selezionare il livello di sicurezza per il FireWall........ 39
5.2.19 Backup: Creazione manuale di backup........ 39
5.2.20 Backup: Creazione di backup automatizzati........ 41

6 Sistema di scansione ... 44

7 Aggiornamenti ... 46

8 Avira FireWall :: Panoramica ... 48

9 Backup ... 51

10 Risoluzione di problemi, suggerimenti ... 52

10.1 Assistenza in caso di problemi ... 52
10.2 Shortcut ... 56
10.2.1 Nelle finestre di dialogo ... 56
10.2.2 Nella Guida in linea ... 57
10.2.3 In Control Center ... 57
10.3 Centro di sicurezza di Windows ... 59
10.3.1 Generale ... 59
10.3.2 Il Centro sicurezza di Windows e il programma Antivir acquistato. ... 59

11 Virus e altro ... 62

11.1 Categorie di minacce ... 62
11.2 Virus e altri malware ... 64

12 Info e Service ... 68

12.1 Indirizzi di contatto ... 68
12.2 Supporto tecnico ... 68
12.3 File sospetto ... 69
12.4 Comunicare un falso allarme ... 69
12.5 Un suo Feedback per una maggiore sicurezza ... 69

13 Riferimento: Opzioni di configurazione ... 70

13.1 Sistema di scansione ... 70
13.1.1 Cerca ... 70
13.1.1.1. Azione per i rilevamenti ... 73
13.1.1.2. Eccezioni ... 75
13.1.1.3. Euristico ... 76
13.1.2 Report ... 77
13.2 Guard ... 78
13.2.1 Cerca ... 78
13.2.1.1. Azione per i rilevamenti ... 80
13.2.1.2. Altre azioni ... 82
13.2.1.3. Eccezioni ... 83
13.2.1.4. Euristico ... 86
13.2.2 ProActiv ... 87
13.2.2.1. Filtro di applicazione: Applicazioni da bloccare ... 88
13.2.2.2. Filtro di applicazione: Applicazioni consentite ... 89
13.2.3 Report ... 90
13.3 MailGuard ... 91
13.3.1 Cerca ... 91
13.3.1.1. Azione per i rilevamenti ... 92
13.3.1.2. Altre azioni ... 93
13.3.1.3. Euristico ... 94
13.3.1.4. AntiBot ... 95
13.3.2 Generale ... 96
13.3.2.1. Eccezioni ... 96
13.3.2.2. Memoria temporanea ... 97

1 Introduzione

Il programma AntiVir protegge efficacemente il computer da virus, worm, trojan, adware e spyware e altri pericoli. In questo manuale vengono brevemente descritti virus o malware (software dannoso) e programmi indesiderati.

La guida descrive l'installazione e il funzionamento del programma.

Sul sito Web Avira sono disponibili numerose opzioni e ulteriori informazioni:

http://www.avira.it

Sul sito Web Avira è possibile...

- Richiamare informazioni su ulteriori programmi AntiVir Desktop
- scaricare il programma AntiVir Desktop più recente
- scaricare il manuale del prodotto più recente in formato PDF
- scaricare strumenti di supporto e riparazione gratuiti
- utilizzare la banca dati completa e gli articoli FAQ relativi alla risoluzione di problemi
- richiamare gli indirizzi di assistenza specifici per paese.

Il team di Avira

2 Simboli ed evidenziazioni

Si utilizzano i seguenti simboli:

Simbolo/Definizione	**Spiegazione**
✓	Esiste un requisito che deve essere soddisfatto prima che sia eseguita un'operazione.
▸	Prima di un'operazione che deve essere eseguita dall'utente.
→	Prima di un evento scaturito dall'operazione precedente.
Attenzione	Prima di un avviso di pericolo di una significativa perdita di dati.
Suggerimenti	Prima di un messaggio con informazioni particolarmente importanti o prima di un suggerimento che agevola la comprensione e l'uso del programma AntiVir.

Si utilizzano le seguenti evidenziazioni:

Evidenziazione	**Spiegazione**
Corsivo	Nome del file o percorso.
	Elementi dell'interfaccia del software che vengono visualizzati (ad esempio titolo della finestra, sezione o campo di opzione).
Grassetto	Elementi dell'interfaccia software, su cui è possibile fare clic (ad es. voci di menu, rubriche o pulsanti).

3 Informazioni sul prodotto

In questo capitolo è possibile ricevere tutte le informazioni importanti per l'acquisto e l'utilizzo del prodotto AntiVir:

– vedere capitolo: Prestazioni
– vedere capitolo: Requisiti di sistema
– vedere capitolo: Licenza
– vedere capitolo:

I programmi AntiVir offrono strumenti completi e flessibili per proteggere efficacemente il computer da virus, malware, programmi indesiderati e altri pericoli.

▶ Prestare attenzione ai seguenti suggerimenti:

Suggerimenti
La perdita di dati importanti ha spesso conseguenze drammatiche. Nemmeno il miglior programma antivirus può offrire una protezione al 100% contro la perdita di dati. Si consiglia di eseguire regolarmente copie di sicurezza (backup) dei dati.

Suggerimenti
Un programma in grado di proteggere il computer da virus, malware, programmi indesiderati e altri pericoli può essere affidabile ed efficace solo se aggiornato regolarmente. Si consiglia di garantire l'aggiornamento del programma AntiVir tramite aggiornamenti automatici. Configurare adeguatamente il programma.

3.1 Prestazioni

Il programma AntiVir dispone delle seguenti funzioni:

– Control Center per il monitoraggio, l'amministrazione e la gestione dell'intero programma
– Configurazione centrale con configurazione semplice in modalità esperto oppure standard e dotata di guida in linea sensibile al contesto
– Scanner (On-Demand Scan) con scansione di tutti i tipi noti di virus e malware gestita dal profilo e configurabile
– Integrazione nella funzionalità di controllo di Windows Vista (Controllo dell'account utente) per poter eseguire operazioni per le quali sono necessari i diritti di amministratore.
– Guard (On-Access Scan) per il costante monitoraggio di tutti gli accessi ai file
– Componente ProActiv per il monitoraggio permanente di azioni eseguite dai programmi (solo per sistemi a 32 bit, non disponibile in Windows 2000)
– MailGuard (sistema di scansione POP3, sistema di scansione IMAP e sistema di scansione SMTP) per il controllo permanente delle email per virus e malware. Verifica estesa degli allegati email

– WebGuard per il monitoraggio dei dati e dei file trasferiti da Internet mediante protocollo HTTP (monitoraggio delle porte 80, 8080, 3128)
– Componente Protezione bambini è provvisto di filtri basati sui ruoli per filtrare pagine Web indesiderate e per limitare il tempo di utilizzo di Internet
– Componente Backup per la creazione di backup dei dati (backup speculari)
– Gestione integrata della quarantena per l'isolamento e il trattamento di file sospetti
– Protezione rootkit per il rilevamento di malware installatisi occultamente nel sistema del computer (i cosiddetti rootkit)
(non disponibile in Windows XP 64 Bit)
– Accesso diretto in Internet a informazioni dettagliate su virus rilevati e malware
– Aggiornamento semplice e rapido del programma, delle definizioni dei virus (VDF) e del motore di ricerca mediante Aggiornamento singolo file e aggiornamento incrementale VDF mediante un server web su Internet
– Licenza facilmente gestibile dall'utente
– integrato per la pianificazione di operazioni singole o ricorrenti come aggiornamenti o scansioni
– Identificazione estremamente precisa di virus e malware per mezzo di tecnologie di ricerca (motore di ricerca) che includono la procedura di ricerca euristica
– Identificazione di tutti i tipi di archivio convenzionali, inclusa l'identificazione di archivi nascosti e Smart-Extension
– Elevata performance grazie alla capacità multi threading (scansione contemporanea di molti file ad alta velocità)
– FireWall Avira per la protezione del computer da accessi non consentiti provenienti da Internet, da una rete o da accessi a Internet/rete da parte di utenti non autorizzati.

3.2 Requisiti di sistema

È necessario soddisfare i seguenti requisiti di sistema::

– Computer a partire dal Pentium, minimo 266 MHz
– Sistema operativo
– Windows XP, SP2 (32 o 64 Bit) o
– Windows Vista (32 o 64 Bit, SP 1)
– Windows 7 (32 o 64 Bit)
– Min. 150 MB di memoria libera sull'hard disk (maggiore quantità di memoria se si utilizza la quarantena e la memoria temporanea)
– Min. 256 MB di memoria principale in Windows XP
– Min. 1024 MB di memoria principale in Windows Vista, Windows 7
– Per l'installazione del programma: diritti di amministratore
– Per tutte le installazioni: Windows Internet Explorer 6.0 o superiore
– Eventuale connessione Internet (vedi Installazione)

3.3 Licenza e aggiornamento

Per poter utilizzare il prodotto AntiVir è necessario possedere una licenza. In questo modo si prende visione delle condizioni di licenza.

La licenza viene assegnata sotto forma di una chiave di attivazione. La chiave di attivazione è un codice alfanumerico che l'utente riceve all'acquisto del prodotto AntiVir. La chiave di attivazione comprende i dati esatti della licenza, ossia quali sono i programmi dotati di licenza e per quale periodo.

Se il programma AntiVir è stato acquistato in internet, l'utente riceverà la chiave di attivazione per email, altrimenti è riportata sulla confezione del prodotto.

Per attivare la licenza del programma, è necessario immettere tale chiave durante l'attivazione del programma. L'attivazione del prodotto può avvenire durante l'installazione. Tuttavia, è possibile attivare il programma AntiVir anche in seguito nel Sistema di gestione delle licenze in Guida in linea::Sistema di gestione delle licenze.

Nel Sistema di gestione delle licenze è possibile avviare un aggiornamento a un prodotto della famiglia AntiVir Desktop: In questo modo non è necessario disinstallare il vecchio prodotto manualmente e installare manualmente il nuovo. Tramite l'aggiornamento dal Sistema di gestione delle licenze immettere nell'apposito campo la chiave di attivazione del prodotto di cui si desidera effettuare l'aggiornamento. Il nuovo prodotto viene installato automaticamente.

Tramite il Sistema di gestione delle licenze è possibile effettuare l'aggiornamento automatico dei seguenti prodotti:

- Aggiornamento di Avira AntiVir Personal ad Avira AntiVir Premium
- Aggiornamento da Avira AntiVir Personal a Avira Premium Security Suite
- Aggiornamento da Avira AntiVir Premium a Avira Premium Security Suite

4 Installazione e disinstallazione

In questo capitolo si ottengono informazioni relative all'installazione e la disinstallazione del programma AntiVir:

- vedere capitolo Installazione: requisiti, modalità di installazione, esecuzione dell'installazione
- vedere capitolo Moduli di installazione
- vedere capitolo Modifica dell'installazione
- vedere capitolo Disinstallazione: esegui disinstallazione

4.1 Installazione

Prima dell'installazione verificare che il computer risponda ai requisiti minimi di sistema. Se il computer soddisfa i requisiti minimi è possibile installare il programma AntiVir.

Suggerimenti
Nel corso della procedura di installazione è possibile creare un punto di ripristino. Un punto di ripristino serve a riportare il sistema operativo allo stato precedente all'installazione. Se si desidera utilizzare questa opzione, assicurarsi che il sistema operativo consenta la creazione di un punto di ripristino:
Windows XP: Proprietà del sistema -> Ripristino del sistema: disattivare l'opzione **Disattiva ripristino del sistema**.
Windows Vista / Windows 7: Proprietà del sistema -> Protezione del sistema: Nella sezione **Impostazioni di protezione** selezionare il drive sul quale è installato il sistema e premere il pulsante **Configura**. Nella finestra **Protezione di sistema** attivare l'opzione **Ripristina le impostazioni di sistema e le precedenti versioni del file**.

Tipi di installazione

Durante l'installazione mediante l'assistente di installazione è possibile selezionare un tipo di setup:

Express

- Non verranno installati tutti i componenti del programma disponibili. I seguenti componenti software non vengono installati:

  Avira AntiVir ProActiv

  Avira FireWall

- I file del programma vengono installati in una directory standard predefinita in `C:\Programmi`.
- Il programma AntiVir verrà installato con le impostazioni standard. È possibile effettuare impostazioni predefinite nell'assistente di configurazione.

Personalizzata

- Si ha la possibilità di selezionare per l'installazione singole componenti del programma (vedi capitolo Installazione e disinstallazione::Moduli di installazione).

- Si può scegliere una cartella di destinazione per i file di programma da installare.
- È possibile disattivare la creazione di un'icona sul desktop e di un gruppo di programmi nel menu di avvio.
- Nella configurazione guidata è possibile effettuare impostazioni predefinite del programma AntiVir e lanciare una breve scansione del sistema, che viene eseguita automaticamente dopo l'installazione.

Prima dell'avvio della procedura di installazione

- Chiudere il programma email. Si consiglia inoltre di chiudere tutte le applicazioni in uso.
- Assicurarsi che non siano installate altre protezioni contro virus. Le funzioni automatiche di protezione di diverse applicazioni antivirus potrebbero entrare in conflitto.
- Stabilire una connessione Internet. La connessione a Internet è necessaria per eseguire i seguenti passaggi dell'installazione:
- Scaricare i file attuali di programma e del motore di ricerca, nonché i file di definizione dei virus aggiornati mediante il programma di installazione (per installazione basata su Internet)
- Attivazione del programma
- Esecuzione di un eventuale aggiornamento a installazione conclusa
- Tenere a portata di mano la chiave di licenza del programma AntiVir, se si desidera attivarlo.

Suggerimenti
Installazione basata su Internet:
per eseguire un'installazione basata su Internet del programma, è disponibile un programma di installazione che carica i file di programma aggiornati prima di eseguire l'installazione dai server Web di Avira GmbH. Tale procedura garantisce l'installazione di AntiVir con un file di definizione dei virus aggiornato.
Installazione con un pacchetto di installazione:
il pacchetto di installazione contiene sia il programma di installazione sia tutti i file di programma necessari. Tuttavia nell'installazione con un pacchetto di installazione non è possibile effettuare la selezione della lingua per il programma AntiVir. Al termine dell'installazione si consiglia di eseguire un aggiornamento del file di definizione dei virus.

Suggerimenti
Per attivare il prodotto, il programma AntiVir comunica tramite il protocollo HTTP e la porta 80 (comunicazione Web), nonché tramite il protocollo di codifica SSL e la porta 443 con i server di Avira GmbH. Se si utilizza un firewall, assicurarsi che la connessione necessaria e i dati in entrata e in uscita non vengano bloccati dal firewall.

Eseguire l'installazione

Il programma di installazione funziona in modalità di dialogo. Ogni finestra contiene una determinata selezione di pulsanti per la gestione del processo di installazione.

I pulsanti principali hanno le seguenti funzioni:

- **OK:** per confermare l'azione.

– **Annulla:** per annullare l'azione.
– **Continua:** per passare alla fase successiva.
– **Indietro:** per passare alla fase precedente.

Installare il programma AntiVir nel modo seguente:

Suggerimenti
Le azioni di seguito descritte per disattivare il firewall di Windows riguardano solo il sistema operativo Windows XP.

▶ Avviare il programma di installazione facendo doppio clic sul file di installazione scaricato da Internet o inserire il CD del programma.

Installazione basata su Internet

→ Appare la finestra di dialogo *Benvenuti...*.

▶ Fare clic su **Avanti** per continuare l'installazione.

→ Appare la finestra di dialogo *Seleziona lingua*.

▶ Selezionare la lingua con cui si desidera installare il programma AntiVir e confermare la scelta con **Continua**.

→ Appare la finestra di dialogo *Download*. Tutti i file necessari per l'installazione vengono scaricati dai server Web di Avira GmbH. Al termine del download la finestra *Download* si chiude.

Installazione con un pacchetto di installazione

→ L'assistente di installazione si apre con la finestra di dialogo *Avira Premium Security Suite*.

▶ Fare clic su *Accetta* per avviare l'installazione.

→ Il file di installazione viene decompresso. La routine di installazione viene avviata.

→ Appare la finestra di dialogo *Benvenuti...*.

▶ Fare clic su **Avanti**.

Prosecuzione dell'installazione basata su Internet o dell'installazione con un pacchetto di installazione

→ Appare ora la finestra di dialogo con l'accordo di licenza.

▶ Confermare l'accettazione della licenza e fare clic su **Avanti**.

→ Appare la finestra di dialogo *Crea numero di serie*.

▶ Confermare, se richiesto, che si è generato un numero di serie casuale che verrà riportato durante l'aggiornamento e fare clic su **Avanti**.

→ Appare la finestra di dialogo*Selezionare modalità di installazione*.

▶ Attivare l'opzione **Express** o **Personalizzata.** Se si desidera creare un punto di ripristino, attivare l'opzione **Crea punto di ripristino del sistema**. Confermare i propri dati con **Avanti**.

Installazione personalizzata

→ Appare la finestra di dialogo *Seleziona directory di destinazione*.

▶ Confermare la directory di destinazione con **Avanti**.

- OPPURE -

Selezionare con **Sfoglia** un'altra directory di destinazione e confermare con **Avanti**.

→ Appare la finestra *Installa i componenti*:

▶ Attivare o disattivare i componenti desiderati e confermare con **Avanti**.

→ Se si sono selezionati i componenti ProActiv per l'installazione, appare la finestra *AntiVir ProActiv Community*. Si ha quindi la possibilità di confermare la propria partecipazione alla community di AntiVir ProActiv: Se l'opzione è attivata, Avira AntiVir ProActiv invia i dati relativi ai programmi sospetti, indicati dai componenti ProActiv, al Centro Ricerca Malware Avira. I dati vengono impiegati unicamente per una più ampia verifica online e per l'ampliamento e il perfezionamento della tecnologia di riconoscimento. Mediante il link **ulteriori informazioni** è possibile richiamare i dettagli della verifica online.

▶ Attivare o disattivare la partecipazione alla AntiVir ProActiv Community e confermare con **Avanti**.

→ Nelle seguenti finestre di dialogo è possibile stabilire se creare o meno un collegamento sul desktop e/o un gruppo di programmi sul menu.

▶ Fare clic su **Avanti**.

▶ Passare alla sezione successiva "Installazione Express".

Installazione Express

→ Compare la finestra *AntiVir ProActiv Community*. Si ha quindi la possibilità di confermare la propria partecipazione alla community di AntiVir ProActiv: Se l'opzione è attivata, Avira AntiVir ProActiv invia i dati relativi ai programmi sospetti, indicati dai componenti ProActiv, al Centro Ricerca Malware Avira. I dati vengono impiegati unicamente per una più ampia verifica online e per l'ampliamento e il perfezionamento della tecnologia di riconoscimento. Mediante il link **ulteriori informazioni** è possibile richiamare i dettagli della verifica online.

▶ Attivare o disattivare la partecipazione alla AntiVir ProActiv Community e confermare con **Avanti**.

Prosecuzione: installazione Express e personalizzata

→ Si apre l'assistente per l'installazione della licenza.

Per attivare il programma sono disponibili le seguenti opzioni

– Immissione di una chiave di attivazione

  Immettendo la chiave di attivazione, il programma AntiVir verrà attivato con la licenza dell'utente.

– Scelta dell'opzione **Prova il prodotto**

  Selezionando **Prova il prodotto**, durante la procedura di attivazione verrà generata una licenza di evaluation con cui viene attivato il programma. È possibile provare il programma AntiVir per un periodo di tempo determinato in tutte le sue funzioni.

Suggerimenti
Tramite l'opzione **File di licenza valido hbedv.key disponibile**, è possibile leggere un file di licenza valido. Il file di licenza viene generato durante la procedura di attivazione del prodotto tramite una chiave di attivazione valida e archiviato nella directory di programma di AntiVir. Utilizzare questa opzione se si è già eseguita l'attivazione del prodotto e si desidera installare nuovamente il programma AntiVir.

Suggerimenti
In alcune versioni in vendita di AntiVir, la chiave di attivazione è già memorizzata nel prodotto. Pertanto non è necessario immettere una chiave di attivazione. In alcuni casi la chiave di attivazione memorizzata viene visualizzata nell'assistente.

Suggerimenti
Per attivare il programma viene stabilita una connessione ai server di Avira GmbH. In **Impostazioni proxy** è possibile configurare la connessione Internet tramite un server proxy.

- Selezionare una procedura di attivazione e confermarla con **Avanti**

Attivazione del prodotto

→ Viene aperta una finestra di dialogo in cui immettere i propri dati personali.

- Immettere i propri dati e fare clic su **Avanti**

→ I dati vengono trasferiti e controllati sui server di Avira GmbH. Il programma AntiVir verrà attivato con la licenza dell'utente.

→ Nella finestra di dialogo seguente vengono visualizzati i dati di licenza dell'utente.

- Fare clic su **Avanti**.
- Saltare la sezione seguente "Attivazione tramite la selezione dell'opzione **hbedv.key valido disponibile** ".

Selezione dell'opzione "hbedv.key valido disponibile"

→ Viene aperta una finestra di dialogo per la lettura del file di licenza.

- Selezionare il file di licenza hbedv.key con i dati di licenza dell'utente per il programma e fare clic su **Apri**

→ Nella finestra di dialogo seguente vengono visualizzati i dati di licenza dell'utente.

- Fare clic su **Avanti**

Prosecuzione dopo la conclusione dell'attivazione o il caricamento del file di licenza

→ I componenti del programma vengono installati. L'avanzamento dell'installazione viene visualizzato nella finestra di dialogo.

→ Nella finestra di dialogo seguente è possibile decidere se, una volta terminata l'installazione, il file readme deve essere aperto e il sistema deve essere riavviato.

- Accettare eventualmente e fare clic su *Fine*per terminare l'installazione.

→ L'assistente di installazione si chiude.

Prosecuzione: Installazione personalizzata
Assistente di configurazione

→ Nell'installazione personalizzata nel passaggio successivo si apre l'assistente di configurazione. Nell'assistente di configurazione è possibile effettuare importanti impostazioni predefinite per il programma AntiVir.

- Fare clic su **Avanti** nella finestra di benvenuto dell'assistente di configurazione per iniziare la configurazione del programma.

→ Nella finestra di dialogo *Configura AHeAD* è possibile selezionare un livello di riconoscimento per la tecnologia AHeAD. Il livello di riconoscimento selezionato viene registrato per l'impostazione della tecnologia AHeAD di Scanner (scansione diretta) e di Guard (scansione in tempo reale).

- Selezionare un livello di riconoscimento e proseguire la configurazione con **Avanti**.

→ Nella finestra di dialogo seguente *Seleziona categorie estese delle minacce* è

possibile adattare le funzioni di protezione del proprio programma AntiVir con la selezione delle categorie delle minacce.

▶ Attivare eventualmente ulteriori categorie delle minacce e proseguire la configurazione con *Avanti*.

→ Nel caso in cui si sia selezionato il modulo di installazione Avira FireWall, appare la finestra di dialogo *Livello di sicurezza FireWall*. È possibile decidere se Avira Firewall può autorizzare l'accesso esterno a risorse condivise nonché l'accesso alla rete di applicazioni di produttori affidabili.

▶ Attivare le opzioni desiderate e proseguire la configurazione con *Avanti*.

→ Nel caso in cui si sia selezionato il modulo di installazione AntiVir Guard, appare la finestra di dialogo *Modalità di avvio Guard*. È ora possibile stabilire il momento in cui avviare Guard. Nella modalità di avvio indicata Guard viene avviato a ogni riavvio del computer.

Suggerimenti
La modalità di avvio indicata di Guard viene memorizzata nel registro e non può essere modificata mediante la configurazione.

▶ Attivare l'opzione desiderata e proseguire la configurazione con *Avanti*.

→ Nel caso in cui si sia selezionato il modulo di installazione AntiVir WebGuard, appare la finestra di dialogo *Attiva protezione bambini*. È ora possibile stabilire il momento in cui avviare Guard. Nella modalità di avvio indicata Guard viene avviato a ogni riavvio del computer. È possibile assegnare diversi ruoli per l'uso di Internet a seconda degli utenti del calcolatore, bambino, adolescente e adulto. Il servizio Protezione bambini può anche essere disattivato.

▶ Attivare le opzioni desiderate per la protezione bambini e proseguire la configurazione con Avanti.

→ Nella finestra di dialogo seguente *Inserisci password*, è possibile proteggere l'accesso alla configurazione con una password. Questa opzione è particolarmente consigliata quando è attiva la protezione bambini.

→ Nella finestra di dialogo seguente *Scansione del sistema* è possibile attivare o disattivare l'esecuzione di una scansione rapida del sistema. La scansione rapida del sistema viene eseguita al termine della configurazione e prima di riavviare il computer, e verifica la presenza di virus e malware nei programmi avviati e nei file di sistema più importanti.

▶ Attivare o disattivare l'opzione *Scansione rapida del sistema* e proseguire la configurazione con *Avanti*.

→ Nella finestra di dialogo seguente è possibile terminare la configurazione con *Fine*.

▶ Fare clic su *Fine* per terminare la configurazione.

→ Le impostazioni indicate e selezionate vengono registrate.

→ Se è attivata l'opzione *Scansione rapida del sistema* si apre la finestra Luke Filewalker. Scanner esegue una scansione rapida del sistema.

Prosecuzione: installazione Express e personalizzata

→ Se nell'ultima installazione mediante assistente è stata selezionata l'opzione **Riavvia computer**, il calcolatore si riavvia.

→ Una volta terminato il riavvio del computer, se nell'installazione mediante assistente è stata selezionata l'opzione **Visualizza Readme.txt**, viene visualizzato il file readme.

Dopo un'installazione riuscita si consiglia in Control Center *Panoramica :: Stato* di verificare l'aggiornamento del programma.

- Se necessario eseguire un aggiornamento per aggiornare il file di definizione dei virus.
- Infine eseguire una scansione completa del sistema.

4.2 Modifiche all'installazione

Si ha la possibilità di aggiungere singoli componenti del programma all'attuale installazione di AntiVir o di rimuoverli (vedere Capitolo Installazione e disinstallazione::Moduli d'installazione)

Se si desidera aggiungere o eliminare componenti del programma dell'installazione corrente, è possibile utilizzare l'opzione **Installazione applicazioni**, **Cambia/Rimuovi programmi** all'interno del **pannello di controllo di Windows**.

Selezionare il programma AntiVir e fare clic su **Modifica**. Nella finestra di dialogo di benvenuto del programma selezionare l'opzione **Modifica programma**. Si è così inseriti nella modifica dell'installazione.

4.3 Moduli di installazione

Nel caso di un'installazione personalizzata o di una modifica di un'installazione è possibile selezionare, aggiungere o eliminare i seguenti moduli:

– **Premium Security Suite**
  Questo modulo contiene tutti i componenti necessari per l'installazione corretta del programma AntiVir.
– **AntiVir Guard**
  AntiVir Guard è in esecuzione in background. Monitora e ripara i file, quando possibile, durante operazioni come apertura, scrittura e copia in tempo reale (On-Access = all'accesso). Se un utente esegue un'operazione (caricamento, esecuzione, copia di un file), il programma AntiVir scansiona automaticamente il file. Durante l'operazione di rinomina del file AntiVir Guard non esegue alcuna scansione.
– **AntiVir ProActiv**
  Il componente ProActiv monitorizza le azioni delle applicazioni e notifica i comportamenti sospetti. Grazie a questo riconoscimento basato sul comportamento è possibile proteggersi dai malware. Il componente ProActiv è integrato in AntiVir Guard.

– **AntiVir MailGuard**
  MailGuard è l'interfaccia tra il computer e il server email da cui il programma di posta (Email-Client) scarica le email. MailGuard funge da cosiddetto Proxy tra il programma email e il server email. Tutte le email in entrata vengono convogliate mediante questo proxy, e, una volta ricercati virus e programmi indesiderati, vengono inoltrate al programma di email. In base alla configurazione il programma tratta le email infette automaticamente o chiede all'utente l'azione da eseguire. Inoltre, MailGuard offre una protezione affidabile contro lo spam.
– **WebGuard AntiVir**
  Durante la navigazione in Internet si richiedono dati da un server Web mediante il browser Web. I dati trasferiti dal server Web (file HTML, file di script e immagini, file flash, file audio e video, ecc.) normalmente passano dalla cache del browser direttamente all'esecuzione nel browser Web cosicché non è possibile una scansione in tempo reale come quella prevista da AntiVir Guard. In questo modo virus e programmi indesiderati potrebbero entrare nel computer. WebGuard è un cosiddetto proxy HTTP che monitora le porte utilizzate per il trasferimento dei dati (80, 8080, 3128) e controlla la presenza di virus e programmi indesiderati nei file trasferiti. In base alla configurazione il programma tratta i file infetti automaticamente o chiede all'utente l'azione da eseguire.
– **Avira FireWall**
  Avira FireWall controlla le vie di comunicazione da e verso il computer. Consente o nega la comunicazione sulla base delle direttive di sicurezza.
– *Protezione rootkit di AntiVir*
  La protezione rootkit di AntiVir controlla se sul computer sono già installati software che dopo l'intrusione nel computer non si riesce a rilevare con i metodi convenzionali del riconoscimento di malware.
– **Shell Extension**
  Le estensioni shell creano nel menu contestuale di Windows Explorer (tasto destro del mouse) la voce Controlla i file selezionati con AntiVir. Con questa voce è possibile scansionare direttamente singoli file o directory.
– **Backup**

Il componente Backup consente di creare manualmente e in modo automatico backup speculari dei dati.

4.4 Disinstallazione

Se si desidera eliminare il programma AntiVir dal proprio computer, è possibile utilizzare l'opzione **Software** in **Cambia/Rimuovi** programmi nelle applicazioni di sistema Windows.

Si può disinstallare il programma AntiVir (descritto ad esempio per Windows XP e Windows Vista) nel seguente modo:

▶ Aprire nel menu **Start** di Windows il **Pannello di controllo**.

▶ Fare doppio clic su **Programmi** (Windows XP: **Software**).

▶ Selezionare il programma AntiVir dall'elenco e fare clic su **Cancella**.

→ Verrà chiesto all'utente se desidera davvero eliminare il programma.

- Confermare con **Sì**.

→ All'utente viene chiesto se deve essere riattivato il firewall di Windows (dal momento che Avira FireWall viene disattivato).

- Confermare con **Sì**.

→ Tutte le componenti del programma vengono eliminate.

- Fare clic su **Fine** per terminare la disinstallazione.

→ Appare una finestra di dialogo con il suggerimento di riavviare il computer.

- Confermare con **Sì**.

→ Il programma AntiVir viene disinstallato, se necessario il computer viene riavviato e tutte le directory, i file e le voci del registro del programma vengono eliminate.

5 Panoramica

In questo capitolo è possibile consultare una panoramica delle funzionalità e del funzionamento del programma AntiVir.

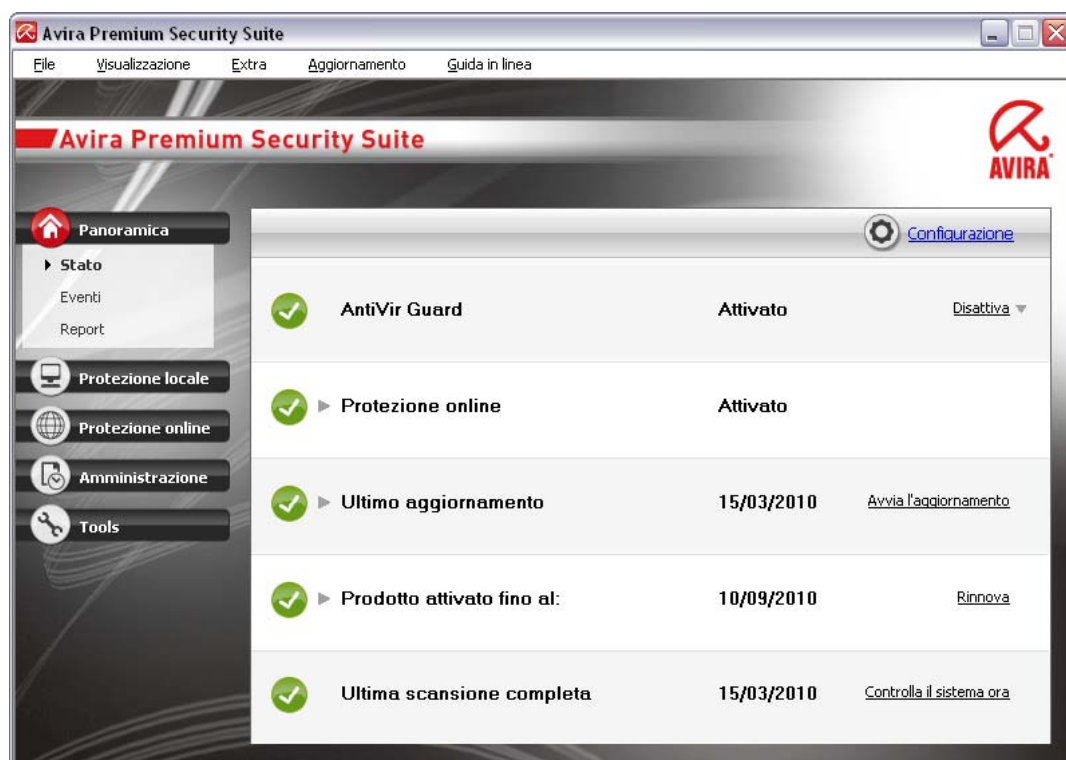
– vedere capitolo Interfaccia e funzionamento
– vedere capitolo Come procedere

5.1 Interfaccia utente e funzionamento

É possibile usare il programma AntiVir mediante tre elementi dell'interfaccia del programma:

– Control Center: Monitoraggio e gestione del programma AntiVir
– Configurazione: Configurazione del programma AntiVir
– Icona Tray della barra delle applicazioni: Apertura di Control Center e altre funzioni

5.1.1 Control Center

Il Control Center serve per il monitoraggio dello stato di protezione del computer e per la gestione e il funzionamento delle componenti di protezione e delle funzioni del programma AntiVir.

La finestra di Control Center è divisa in tre sezioni: l'**elenco menu** , la **barra di navigazione** e la finestra per i dettagli **Visualizza**:

– **Elenco menu:** nei menu di Control Center è possibile richiamare funzioni generali e informazioni del programma.
– **Sezione di navigazione:** nella sezione di navigazione è possibile passare in modo semplice da una rubrica all'altra di Control Center. Le singole rubriche contengono informazioni e funzioni delle componenti del programma e sono presenti sulla barra di navigazione in base alle sezioni dei task. Esempio: sezione dei task *Panoramica* - Rubrica **Stato**.
– **Visualizza:** in questa finestra viene visualizzata la categoria che è stata selezionata nella sezione di navigazione. In base alla rubrica nella barra superiore della finestra dei dettagli sono presenti pulsanti per l'esecuzione di funzioni o azioni. Nelle singole rubriche vengono visualizzati dati o oggetti presenti negli elenchi. É possibile ordinare le liste facendo clic sul campo in base al quale si desidera ordinare le stesse.

Avvio e chiusura di Control Center

Per avviare Control Center è possibile scegliere tra le seguenti modalità:

– fare doppio clic sull'icona del programma sul desktop
– mediante la voce del programma nel menu Start | Programmi.
– mediante l'Icona Tray del programma AntiVir.

Si può chiudere Control Center mediante il comando **Chiudi** nel menu **File** o facendo clic sulla x nella finestra di Control Center.

Utilizzo di Control Center

Come navigare in Control Center

▶ Selezionare una sezione dei task nella barra di navigazione.

→ La sezione dei task si apre e appaiono diverse rubriche. La prima rubrica della sezione dei task viene selezionata e visualizzata.

▶ Fare clic su un'altra categoria per visualizzarla nella finestra dei dettagli.

- OPPURE -

▶ Selezionare una rubrica mediante il menu *Visualizza*.

Suggerimenti
Attivare la navigazione da tastiera nell'elenco menu con l'ausilio del tasto [Alt]. Se la navigazione con tastiera è attivata, è possibile spostarsi all'interno dei menu con i tasti freccia. Con il tasto Invio si attiva la voce di menu selezionata in quel momento.
Per aprire, chiudere o navigare nei menu di Control Center è possibile utilizzare anche le combinazioni di tasti: tasto [Alt] + lettera sottolineata nel menu o nel comando. Tenere premuto il tasto [Alt] se si desidera richiamare un comando o un sottomenu dal menu.

Come elaborare dati o oggetti che vengono visualizzati nella finestra dei dettagli:

▶ Evidenziare i dati o gli oggetti che si desidera elaborare.

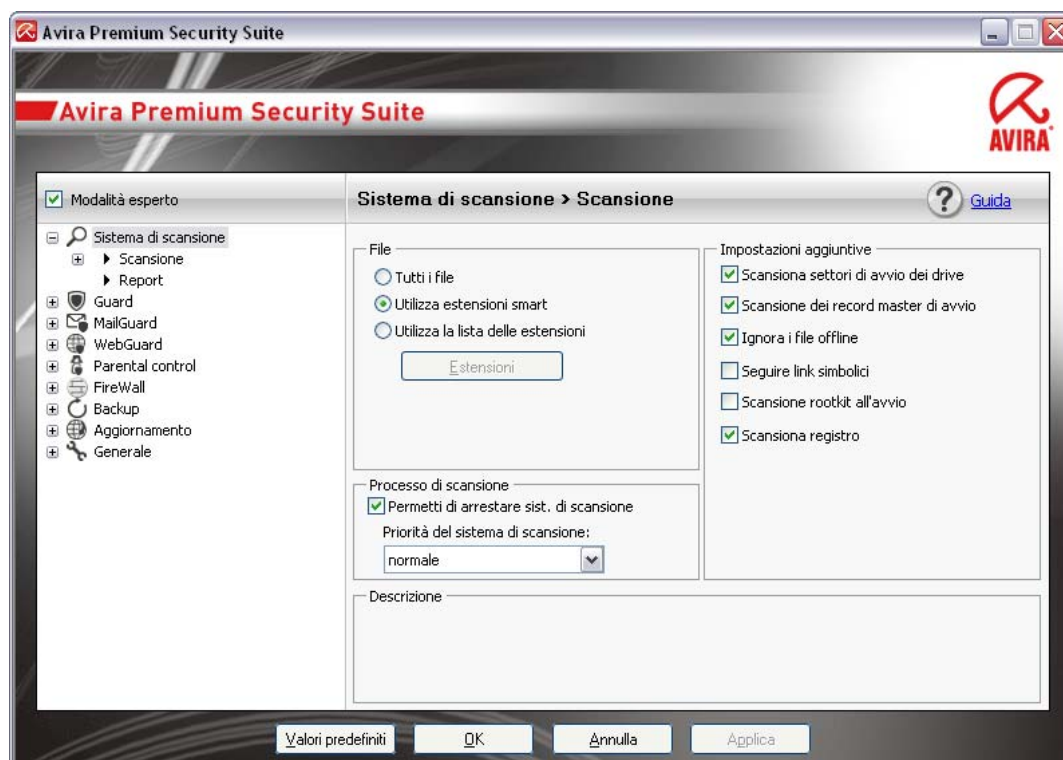
Per evidenziare più elementi, tenere premuto il tasto Ctrl o il tasto Shift (selezione di elementi consecutivi) durante la selezione degli elementi.

▶ Fare clic sui pulsanti desiderati nella barra superiore della finestra dei dettagli per elaborare l'oggetto.

Control Center in sintesi

– **Panoramica**: in **Panoramica** sono disponibili tutte le rubriche che consentono di monitorare le funzionalità del programma AntiVir.
– La rubrica **Stato** offre la possibilità di visualizzare quali moduli del programma sono attivi e fornisce informazioni sull'ultimo aggiornamento effettuato. Inoltre, è possibile verificare se si possiede una licenza valida.
– La rubrica Eventi consente di ottenere informazioni sugli eventi generati dai moduli del programma.
– La rubrica Report consente di visualizzare i risultati delle azioni eseguite.
– **Protezione locale**: in **Protezione locale** sono disponibili i componenti con cui eseguire la ricerca di virus e malware nei file del computer.
– La rubrica Scansiona offre la possibilità di configurare o avviare la scansione diretta in modo semplice. I profili predefiniti consentono una scansione con le opzioni standard già adeguate. Con l'aiuto della Selezione manuale (non viene memorizzata) o con la creazione di un Profilo definito dall'utente, è possibile adattare la scansione di virus e programmi indesiderati alle proprie esigenze personali.
– La rubrica Guard visualizza informazioni su file scansionati, così come ulteriori dati statistici, che possono essere ripristinati in qualsiasi momento e permette il richiamo del file di report. È possibile ottenere Informazioni dettagliate sui virus e programmi indesiderati "premendo un pulsante".
– **Protezione online**: in **Protezione online** sono disponibili i componenti che consentono di proteggere il computer da virus e malware provenienti da Internet, nonché da accessi di rete indesiderati.
– La rubrica MailGuard mostra le email verificate da MailGuard, le loro proprietà e altri dati statistici. Inoltre, si ha la possibilità di spostare il filtro AntiSpam ed escludere indirizzi email dalla scansione per malware o spam. Le email possono essere eliminate anche dalla memoria temporanea di MailGuard.
– La rubrica WebGuard visualizza informazioni sugli URL scansionati e sui virus individuati, nonché ulteriori dati statistici che possono essere ripristinati in qualsiasi momento e consente di richiamare il file di report. È possibile ottenere Informazioni dettagliate sui virus e programmi indesiderati "premendo un pulsante".
– La rubrica FireWall offre la possibilità di configurare le impostazioni di base di Avira FireWall. Vengono inoltre visualizzate le attuali velocità di trasferimento dati e tutte le applicazioni attive che utilizzano un collegamento alla rete.
– **Gestione**: in **Gestione** sono disponibili gli strumenti che consentono di isolare e gestire file sospetti o infetti nonché pianificare attività ricorrenti.
– Nella rubrica Quarantena è disponibile il cosiddetto Gestore della quarantena: la postazione centrale per i file già in quarantena o per file sospetti che si desidera spostare in quarantena. Inoltre esiste la possibilità di inviare un file selezionato per email all'Avira Malware Research Center.
– La rubrica Pianificatore offre la possibilità di creare job temporizzati di controllo e di aggiornamento nonché di backup e di cancellare o modificare job esistenti.
– **Strumenti**: in **Strumenti** sono disponibili ulteriori strumenti per la sicurezza dei dati.
– Nella rubrica Backup è possibile creare in modo semplice e rapido i backup dei dati e assegnare i job di backup.

5.1.2 Configurazione

In Configurazione è possibile effettuare le impostazioni per il programma AntiVir . Dopo l'installazione, il programma AntiVir è configurato con le impostazioni standard che assicurano la protezione ottimale del computer. Ciononostante, il computer o le richieste dell'utente per il programma AntiVir possono possedere caratteristiche particolari e richiedere un adattamento delle componenti di protezione del programma.

La configurazione dispone di una finestra di dialogo: con i pulsanti OK o Applica si memorizzano le impostazioni scelte durante la configurazione, con Annulla si rifiutano le impostazioni, con il pulsante Valori standard è possibile ripristinare le impostazioni dei valori standard della configurazione. Nella barra di navigazione a sinistra è possibile selezionare singole rubriche di configurazione.

Richiamo della Configurazione

Esistono diverse possibilità per richiamare la configurazione:

– Mediante il Pannello di controllo di Windows.

– Mediante il centro sicurezza di Windows - a partire da Windows XP Service Pack 2.

– mediante l'Icona Tray del programma AntiVir.

– Nel Control Center mediante la voce di menu Extra | Configurazione.

– Nel Control Center mediante il pulsante Configurazione.

Suggerimenti
Se si richiama la configurazione con il pulsante **Configurazione** in Control Center, si giunge nel registro di configurazione della categoria attiva in Control Center. Per selezionare un singolo registro di configurazione, è necessario attivare la modalità esperto della configurazione. In questo caso appare una finestra di dialogo, in cui viene richiesto di attivare la modalità esperto.

Utilizzo della Configurazione

All'interno della finestra di configurazione si può navigare come in Esplora risorse di Windows:

- ▶ Fare clic su una voce della struttura ad albero per visualizzare questa categoria di configurazione nella finestra dei dettagli.
- ▶ Fare clic sul segno + prima delle voci per estendere la categoria di configurazione e visualizzare le rubriche di configurazione subordinate nella struttura ad albero.
- ▶ Per nascondere le rubriche di configurazione subordinate fare clic sul segno - prima della categoria di configurazione estesa.

Suggerimenti
Per attivare o disattivare le opzioni nella configurazione e per premere i pulsanti è possibile utilizzare anche le seguenti combinazioni di tasti: tasto [Alt] + lettera sottolineata nei nomi opzione o nella definizione pulsanti.

Suggerimenti
Le rubriche di configurazione vengono visualizzate per intero nella modalità esperto. Attivare la modalità esperto per visualizzare tutte le rubriche di configurazione. La modalità esperto può essere protetta con una password da digitare al momento dell'attivazione.

Se si desidera registrare le impostazioni nella configurazione:

▶ Fare clic sul pulsante **OK**.

→ La finestra di configurazione viene chiusa e le impostazioni registrate.

- OPPURE -

▶ Fare clic sul pulsante **Applica**.

→ Le impostazioni vengono registrate. La finestra di configurazione rimane aperta.

Se si desidera terminare la configurazione senza memorizzare le impostazioni:

▶ Fare clic sul pulsante **Annulla**.

→ La finestra di configurazione si chiude e le impostazioni vengono ignorate.

Se si desidera ripristinare tutte le impostazioni dei valori standard nella configurazione:

▶ Fare clic su **Valori standard**.

→ Tutte le impostazioni dei valori standard nella configurazione vengono ripristinate. Quando si ripristinano i valori standard tutte le modifiche e le immissioni dell'utente vengono perse.

Opzioni di configurazione in sintesi

Esistono le seguenti opzioni di configurazione:

– **Sistema di scansione**: Configurazione della scansione diretta

Opzioni di ricerca

Azioni in caso di rilevamento

Opzioni per la scansione degli archivi

Eccezioni della scansione diretta

Euristica della scansione diretta

Impostazione della funzione di report

– **Guard**: Configurazione della scansione in tempo reale

Opzioni di ricerca

Azioni in caso di rilevamento

Eccezioni della scansione in tempo reale

Euristica della scansione in tempo reale

Impostazione della funzione di report

– **MailGuard**: configurazione di MailGuard

Opzioni di ricerca: attivazione del monitoraggio degli account POP3, account IMAP, email in uscita (SMTP)

Azioni in caso di malware

Euristica della scansione di MailGuard

Funzione AntiBot: server SMTP consentiti, mittenti email consentiti

Eccezioni della scansione di MailGuard

Configurazione della memoria temporanea, svuota la memoria temporanea

Configurazione della banca dati training AntiSpam, svuota la banca dati training

Configurazione di un piè di pagina nelle email inviate

Impostazione della funzione di report

– **WebGuard**: configurazione di WebGuard

Opzioni di ricerca, attivazione e disattivazione di WebGuard

Azioni in caso di rilevamento

Accesso bloccato: Tipi di file e tipi di MIME indesiderati, Filtro web per URL noti indesiderati (malware, phishing ecc.)

Eccezioni della scansione di WebGuard: URL, tipi di dati, tipi di MIME

Euristica di WebGuard

Funzione Protezione bambini: filtro basato sui ruoli e limitazione temporale dell'utilizzo di Internet basata sui ruoli

Impostazione della funzione di report

– **FireWall**: configurazione del FireWall

Impostazione delle regole adattatore

Impostazione personalizzata delle regole di applicazione

Elenco produttori affidabili (eccezioni per l'accesso di rete delle applicazioni)

Impostazioni avanzate: timeout per le regole, limitazione per file host di Windows, blocco del FireWall di Windows, notifiche

Impostazioni pop up (avvisi per l'accesso di rete delle applicazioni)

– **Backup**:

Impostazione del componente Backup (backup incrementale, scansione di virus durante il backup)

Eccezioni: impostazione dei file da proteggere

Impostazione della funzione di report

– **Generale**:

Categorie estese delle minacce per la scansione diretta e in tempo reale

Protezione password per l'accesso al Control Center e alla configurazione

Sicurezza: indicatore di stato aggiornamento, indicatore di stato scansione completa del sistema, protezione del prodotto

WMI: attiva supporto WMI

Configurazione del log eventi

Configurazione delle funzioni di report

Impostazione delle directory utilizzate

Aggiornamento: configurazione del collegamento al server di download, impostazione dell'aggiornamento del prodotto

Configurazione degli avvisi acustici in caso di rilevamento malware

5.1.3 Icona Tray

Dopo l'installazione, l'icona Tray del programma AntiVir è collocata nella barra delle applicazioni:

Simbolo	Descrizione
	AntiVir Guard è attivato e il FireWall è attivato
	AntiVir Guard è disattivato oppure il FireWall è disattivato

L'icona Tray mostra lo stato del servizio Guard e FireWall.

Le funzioni principali del programma AntiVir sono facilmente accessibili mediante il menu contestuale dell'icona Tray. Per richiamare il menu contestuale, fare clic con il tasto destro del mouse sull'icona Tray.

Voci del menu contestuale

– **Attiva AntiVir Guard**: Attiva o disattiva AntiVir Guard.

– **Attiva AntiVir MailGuard**: Attiva o disattiva AntiVir MailGuard.

– **Attiva AntiVir WebGuard**: Attiva o disattiva AntiVir WebGuard.

– **FireWall**:

– Attiva FireWall: attiva o disattiva il FireWall

– Blocca tutto il traffico: Attivata: blocca ogni trasferimento dati con l'eccezione dei trasferimenti al proprio sistema (Local Host / IP 127.0.0.1).

– Attiva modalità di riproduzione: attiva o disattiva la modalità:
Attivato: vengono utilizzate tutte le regole di applicazione e le regole definite per l'adattatore. Viene consentito l'accesso alle applicazioni per le quali non è stata definita alcuna regola e non viene aperta nessuna finestra pop-up.

– **Avvia AntiVir**: Apre il Control Center.

– **Configura AntiVir**: Apre Configurazione.
– **Avvia aggiornamento**: Avvia un aggiornamento.
– **Guida in linea**: Apre la Guida in linea.
– **Informazioni su Premium Security Suite:** Apre una finestra di dialogo con informazioni sul proprio programma AntiVir: Informazioni su prodotto, versione e licenza.
– **Avira su Internet**: Apre il portale Web di Avira in Internet. Il prerequisito essenziale è l'accesso attivo a Internet.

5.2 Come procedere

5.2.1 Attiva il prodotto

Per attivare AntiVir sono disponibili le seguenti opzioni:

– Attivazione con una licenza completa valida

Per attivare il programma con una licenza completa, è necessario disporre di una chiave di attivazione valida che comprende i dati della licenza acquistata. La chiave di attivazione è stata inviata per email oppure è indicata sulla confezione del prodotto.

– Attivazione con una licenza di evaluation

Il programma AntiVir viene attivato tramite una licenza di evaluation generata automaticamente che consente all'utente di testare AntiVir e tutte le relative funzioni per un periodo di tempo limitato.

Suggerimenti
Per attivare il prodotto o richiedere una licenza di prova, è necessario disporre di una connessione Internet attiva.
Nel caso non sia possibile stabilire una connessione ai server di Avira GmbH, controllare eventualmente le impostazioni del firewall utilizzato: durante l'attivazione del prodotto vengono utilizzate connessioni tramite il protocollo HTTP e la porta 80 (comunicazione Web) e tramite il protocollo di codifica SSL e la porta 443. Assicurarsi che il proprio firewall non blocchi i dati in entrata o in uscita. Controllare inoltre che il proprio browser Web sia in grado di richiamare pagine Web.

Attivare il programma AntiVir nel modo seguente:

Se il programma AntiVir non è ancora stato installato:

▶ installare il programma AntiVir.

→ Durante l'installazione viene richiesto all'utente di selezionare un'opzione di attivazione

– *Attiva il prodotto*

= attivazione con una licenza completa valida

– *Prova il prodotto*

= attivazione con una licenza di evaluation

▶ Per l'attivazione con una licenza completa, inserire la chiave di attivazione.

- Confermare la scelta della procedura di attivazione con **Avanti**.
- Inserire eventualmente i propri dati personali per la registrazione e confermare con **Avanti**.

→ Nella finestra di dialogo seguente vengono visualizzati i dati di licenza dell'utente. Il programma AntiVir è stato attivato.

- Continuare l'installazione.

Se il programma AntiVir è già stato installato:

- in Control Center selezionare la voce di menu **Guida in linea :: Gestione delle licenze**.

→ Verrà avviato l'assistente per l'installazione della licenza, con cui è possibile selezionare un'opzione di attivazione. I passaggi successivi per l'attivazione del prodotto sono analoghi alla procedura descritta in precedenza.

5.2.2 Eseguire gli aggiornamenti automatici

Con la seguente procedura è possibile impostare con lo scheduler AntiVir un job con cui aggiornare automaticamente il programma AntiVir:

- In Control Center selezionare la rubrica **Gestione :: Scheduler**.
- Fare clic sul simbolo *Crea nuovo job con wizard*.

→ Appare la finestra di dialogo *Nome e descrizione del job*.

- Assegnare un nome al job e descriverlo.
- Fare clic su **Avanti**.

→ Viene visualizzata la finestra di dialogo *Tipo di job*.

- Selezionare un **Job di aggiornamento** dalla lista.
- Fare clic su **Avanti**.

→ Apparirà la finestra di dialogo *Durata del job*.

- Selezionare quando deve essere eseguita la scansione:
  - **Immediato**
  - **Giornaliero**
  - **Settimanale**
  - **Intervallo**
  - **Unico**
  - **Login**

Suggerimenti
Raccomandiamo di eseguire gli aggiornamenti periodicamente e con una certa frequenza. L'intervallo di aggiornamento consigliato è: 2 Ore.

- Indicare il termine in base alla selezione.
- Selezionare una delle seguenti opzioni aggiuntive (disponibili in base al tipo di job):
  - **Avvia job se è presente una connessione Internet**

Oltre alla frequenza stabilita il job viene eseguito quando si attiva una connessione a Internet.

– **Ripeti job se il tempo è già scaduto**

Vengono eseguiti job scaduti che non è stato possibile eseguire al momento designato, ad esempio perché il computer era spento.

▶ Fare clic su **Avanti**.

→ Appare la finestra di dialogo *Selezione della modalità di visualizzazione*.

▶ Selezionare la modalità di visualizzazione della finestra del job:

– **Ridotta**: solo la barra di progressione

– **Estesa**: tutta la finestra del job

– **Invisibile**: nessuna finestra del job

▶ Fare clic su **Fine**.

→ Il nuovo job assegnato viene visualizzato alla pagina iniziale della rubrica **Gestione :: Verifica** come attivata (segno di spunta).

▶ Disattivare i job che non devono essere eseguiti.

Mediante i seguenti simboli, è possibile elaborare ulteriormente i job:

Visualizza le proprietà di un job

Modifica job

Elimina job

Avvia job

Arresta job

5.2.3 Avvio di un aggiornamento manuale

Sono disponibili varie opzioni per avviare manualmente un aggiornamento: durante gli aggiornamenti avviati manualmente viene sempre eseguito anche l'aggiornamento del file di definizione dei virus e del motore di ricerca. L'aggiornamento del prodotto avviene solo se nella configurazione in Generale :: Aggiornamento è stata selezionata l'opzione **Scarica aggiornamenti prodotto e installa automaticamente**.

L'aggiornamento manuale del programma AntiVir può essere avviato nel modo seguente:

▶ fare clic con il tasto destro del mouse sull'icona Tray di AntiVir nella barra delle applicazioni.

→ Apparirà un menu contestuale.

▶ Selezionare **Avvia aggiornamento**.

→ Appare la finestra di dialogo *Updater*.

- OPPURE -

▶ In Control Center selezionare la rubrica **Panoramica :: Stato**.

- Fare clic nella sezione *Ultimo aggiornamento* sul link **Avvia aggiornamento**.
- → Appare la finestra di dialogo Updater.

- OPPURE -

- In Control Center, nel menu **Aggiornamento** selezionare il comando *Avvia aggiornamento*.
- → Appare la finestra di dialogo Updater.

Suggerimenti
Raccomandiamo di eseguire gli aggiornamenti automatici periodicamente. L'intervallo di aggiornamento consigliato è: 2 Ore.

Suggerimenti
É possibile eseguire un aggiornamento anche manualmente mediante il Centro di sicurezza Windows.

5.2.4 Scansione diretta: Eseguire il controllo di virus e malware con un profilo di ricerca

Un profilo di ricerca è un insieme di drive e directory che devono essere scansionati.

Per effettuare una scansione con un profilo di ricerca è possibile:

– Utilizzare il profilo di ricerca predefinito

Se i profili di ricerca predefiniti si adattano alle proprie esigenze.

– Modificare il profilo di ricerca e utilizzarlo (selezione manuale)

Se si desidera eseguire una scansione con un profilo di ricerca personalizzato.

– Creare e utilizzare un nuovo profilo

Se si desidera salvare un profilo di ricerca personale.

In base al sistema operativo sono disponibili diversi simboli per l'avvio di un profilo di ricerca:

– In Windows XP e 2000:

 Con questo simbolo si avvia la scansione mediante un profilo di ricerca.

– In Windows Vista:

In Microsoft Windows Vista il Control Center ha inizialmente diritti limitati ad esempio per l'accesso a file e directory. Alcune azioni e l'accesso ai file possono essere eseguiti dal Control Center solo con diritti di amministratore avanzati. Questi diritti di amministratore avanzati devono essere assegnati a ogni avvio di una scansione mediante un profilo di scansione.

Con questo simbolo si avvia una scansione limitata mediante un profilo di ricerca. Vengono scansionati solo i file e le directory per cui Windows Vista ha concesso i diritti di accesso.

Con questo simbolo si avvia una scansione con diritti avanzati dell'amministratore. Dopo una conferma, vengono scansionati tutti i file e le directory del profilo di ricerca selezionato.

Per cercare virus e malware con un profilo:

▶ In Control Center selezionare la rubrica **Protezione locale :: Verifica**.

→ Appaiono i profili di ricerca predefiniti.

▶ Selezionare un profilo di ricerca predefinito.

- OPPURE -

▶ Modificare il profilo di ricerca *Selezione manuale*.

- OPPURE -

▶ Creare un nuovo profilo di ricerca

▶ Fare clic sul simbolo (Windows XP: o Windows Vista:).

▶ Appare la finestra *Luke Filewalker* e si avvia la scansione diretta.

→ Al termine del processo di scansione vengono visualizzati i risultati.

Se si desidera modificare un profilo di ricerca:

▶ Aprire in **Selezione manuale** la struttura dei file fin quando non vengono aperti tutti i drive e le directory che devono essere scansionati.

– Fare clic sul segno **+**: viene visualizzato il livello della directory.

– Fare clic sul segno **-**: viene nascosto il livello della directory.

▶ Selezionare i punti e le directory che devono essere scansionati facendo clic nella rispettiva casella dei vari livelli di directory.

Si hanno le seguenti possibilità per selezionare le directory:

– Directory incluse le sottodirectory (segno di spunta nero)

– Directory escluse le sottodirectory (segno di spunta verde)

– Solo le sottodirectory in una directory (segno di spunta grigio, le sottodirectory hanno un segno di spunta nero)

– Nessuna directory (nessun segno di spunta)

Se si desidera creare un nuovo profilo di ricerca:

▶ Fare clic sul simbolo **Crea nuovo profilo**.

→ Il *Nuovo profilo* appare tra quelli già esistenti.

▶ Assegnare un nome al profilo di ricerca con un clic sul simbolo .

▶ Evidenziare altri punti e directory che devono essere verificati con un clic nella casella del livello della directory.

Si hanno le seguenti possibilità per selezionare le directory:

– Directory incluse le sottodirectory (segno di spunta nero)

– Directory escluse le sottodirectory (segno di spunta verde)

– Solo le sottodirectory in una directory (segno di spunta grigio, le sottodirectory hanno un segno di spunta nero)

– Nessuna directory (nessun segno di spunta)

5.2.5 Scansione diretta: Ricerca di virus e malware con Drag & Drop

È possibile cercare con Drag & Drop virus e malware nel modo seguente:

✓ Il Control Center del programma AntiVir è aperto.

- Selezionare il file o la directory, che si desidera controllare.
- Trascinare con il tasto sinistro del mouse il file selezionato o la directory in *Control Center*.

→ Appare la finestra *Luke Filewalker* e si avvia la scansione diretta.

→ Al termine del processo di scansione vengono visualizzati i risultati.

5.2.6 Scansione diretta: Cerca virus e malware con il menu contestuale

Per cercare in maniera mirata virus e malware mediante il menu contestuale:

- Fare clic (ad esempio in Esplora risorse di Windows, sul desktop o in una directory aperta di Windows) con il tasto destro del mouse sul file o sulla directory che si desidera controllare.

→ Appare il menu contestuale di Esplora risorse di Windows.

- Nel menu contestuale selezionare **Controlla i file selezionati con AntiVir**.

→ Appare la finestra *Luke Filewalker* e si avvia la scansione diretta.

→ Al termine del processo di scansione vengono visualizzati i risultati.

5.2.7 Scansione diretta: cerca automaticamente virus e malware

Suggerimenti
Una volta eseguita l'installazione il job *Scansione completa del sistema* si trova nello : in un intervallo di aggiornamento consigliato viene eseguita automaticamente una scansione completa del sistema.

Cercare automaticamente virus e malware è un job che si imposta come segue:

- In Control Center selezionare la rubrica **Gestione :: Scheduler**.
- Fare clic sul simbolo .

→ Appare la finestra di dialogo *Nome e descrizione del job*.

- Assegnare un nome al job e descriverlo.
- Fare clic su **Avanti**.

→ Appare la finestra di dialogo *Tipo di job*.

- Selezionare il **Job di scansione**.
- Fare clic su **Avanti**.

→ Appare la finestra di dialogo *Selezione del profilo*.

- Selezionare quale profilo deve essere scansionato.

- Fare clic su **Avanti**.

→ Apparirà la finestra di dialogo *Durata del job*.

- Selezionare quando deve essere eseguita la scansione:
  - **Immediato**
  - **Giornaliero**
  - **Settimanale**
  - **Intervallo**
  - **Unico**
  - **Login**
- Indicare il termine in base alla selezione.
- Selezionare una delle seguenti opzioni aggiuntive (disponibili in base al tipo di job):
  - **Ripeti job se il tempo è già scaduto**

    Vengono eseguiti job scaduti che non è stato possibile eseguire al momento designato, ad esempio perché il computer era spento.
- Fare clic su **Avanti**.

→ Appare la finestra di dialogo *Selezione della modalità di visualizzazione*.

- Selezionare la modalità di visualizzazione della finestra del job:
  - **Ridotta**: solo la barra di progressione
  - **Estesa**: tutta la finestra del job
  - **Invisibile**: nessuna finestra del job
- Selezionare l'opzione *Spegni computer*, se si desidera che il calcolatore si spenga automaticamente non appena il job è stato eseguito e concluso. L'opzione è disponibile solo nella modalità di visualizzazione ridotta o estesa.
- Fare clic su **Fine**.

→ Il nuovo job assegnato viene visualizzato alla pagina iniziale della rubrica *Gestione :: Scheduler* come attivato (segno di spunta).

- Disattivare i job che non devono essere eseguiti.

Mediante i seguenti simboli, è possibile elaborare ulteriormente i job:

 Visualizza proprietà di un job

 Modifica job

 Elimina job

 Avvia job

 Arresta job

5.2.8 Scansione diretta: Effettuare una scansione mirata per rootkit attivi

Per effettuare una ricerca di rootkit attivi, utilizzare il profilo di ricerca predefinito *Cerca rootkit e malware attivi*.

La ricerca di rootkit mirata si effettua nel modo seguente:

▶ In Control Center selezionare la rubrica **Protezione locale :: Verifica**.

→ Appaiono i profili di ricerca predefiniti.

▶ Selezionare il profilo di ricerca predefinito **Cerca rootkit e malware attivi**.

▶ Evidenziare altri punti e directory che devono essere verificati con un clic nella casella del livello della directory.

▶ Fare clic sul simbolo (Windows XP: o Windows Vista:).

→ Appare la finestra *Luke Filewalker* e si avvia la scansione diretta.

→ Al termine del processo di scansione vengono visualizzati i risultati.

5.2.9 Reagire a virus e malware riscontrati

Per i singoli componenti di protezione del programma AntiVir, è possibile impostare nella configurazione, nella rubrica *Azione in caso di rilevamento* come deve reagire al rilevamento di un virus o di un programma indesiderato.

Nel componente ProActiv di Guard non esiste la possibilità di configurare alcuna opzione di azione: Un rilevamento viene sempre comunicato nella finestra *Guard: Comportamento sospetto di un'applicazione*.

Opzioni di azione in Scanner:

– **Interattivo**

Nella modalità di azione interattiva vengono notificati i rilevamenti della scansione di Scanner in una finestra di dialogo. Questa opzione è attivata di default.
Al termine della **scansione di Scanner**, si riceve un avviso con l'elenco dei file infetti rilevati. Mediante il menu contestuale è possibile selezionare un'azione da eseguire per i singoli file infetti. È possibile eseguire l'azione selezionata per tutti i file infetti oppure interrompere la scansione.

– **Automatico**

Nella modalità di azione automatica, in caso di rilevamento di un virus o di un programma indesiderato l'azione selezionata dall'utente in questa sezione viene eseguita automaticamente.

Opzioni di azione in Guard:

– **Interattivo**

Nella modalità di azione interattiva viene negato l'acceso ai dati e sul desktop viene visualizzato un messaggio. È possibile rimuovere il malware rilevato direttamente nel messaggio sul desktop, oppure trasmetterlo al componente Scanner per un ulteriore trattamento del virus selezionando il pulsante 'Dettagli'. Il sistema di scansione segnala il rilevamento in una finestra, nella quale, mediante un menu contestuale, sono disponibili diverse opzioni per il trattamento del file infetto (vedere Rilevamento::Scanner).

– **Automatico**

Nella modalità di azione automatica, in caso di rilevamento di un virus o di un programma indesiderato, l'azione selezionata dall'utente in questa sezione viene eseguita automaticamente.

Opzioni di azione in MailGuard, WebGuard:

– **Interattivo**

Nella modalità di azione interattiva, in caso di rilevamento di un virus o di un programma indesiderato appare una finestra di dialogo nella quale è possibile scegliere come gestire i file infetti. Questa opzione è attivata di default.

– **Automatico**

Nella modalità di azione automatica, in caso di rilevamento di un virus o di un programma indesiderato l'azione selezionata dall'utente in questa sezione viene eseguita automaticamente.

Nella modalità di azione interattiva si reagisce ai virus e ai programmi indesiderati rilevati selezionando nell'avviso un'azione per gli oggetti infetti ed eseguendo l'azione selezionata mediante conferma.

Per il trattamento di oggetti infetti possono essere selezionate le seguenti azioni:

Suggerimenti
Le azioni disponibili dipendono dal sistema operativo, dal componente di protezione (AntiVir Guard, AntiVir Scanner, AntiVir MailGuard, AntiVir WebGuard) che segnala il file rilevato, e dal malware rilevato.

Azioni del sistema di scansione e del Guard (senza rilevamenti di ProActiv):

– **Ripara**

Il file viene riparato.

Questa opzione è attivabile solo se è possibile riparare il file.

– **Sposta in quarantena**

Il file viene compresso in un formato speciale (**.qua*) e spostato nella directory di quarantena *INFECTED* sull'hard disk, in modo da escludere qualsiasi accesso diretto. I file in questa directory possono essere successivamente riparati nella quarantena o, se necessario, inviati ad Avira GmbH.

– **Elimina**

Il file viene eliminato. Questa procedura è più rapida di *Sovrascrivi ed elimina*. Se il file rilevato è un virus del record di avvio eliminarlo con Elimina. Viene scritto un nuovo record di avvio.

– **Sovrascrivi ed elimina**

Il file viene sovrascritto con un modello e, infine, eliminato. Il file non può essere ripristinato.

– **Rinomina**

Il file viene rinominato **.vir*. Non sarà quindi più possibile accedere direttamente ai file (ad esempio con un doppio clic). I file possono essere successivamente riparati e nuovamente rinominati.

– **Ignora**

Non viene eseguita alcuna altra azione. Il file infetto rimane attivo sul computer.

Attenzione
Pericolo di perdita di dati e danni al sistema operativo! Utilizzare l'opzione *Ignora* solo in casi eccezionali e fondati.

– **Ignora sempre**

Opzione di azione in caso di file rilevati da Guard: Guard non esegue alcuna altra azione. L'accesso al file viene autorizzato. Vengono autorizzati tutti gli accessi successivi a questo file e non si ricevono comunicazioni fino al riavvio del computer o a un aggiornamento del file di definizione dei virus.

– **Copia in quarantena**

Opzione di azione in caso di rilevamento di un rootkit: il file rilevato viene copiato nella quarantena.

– **Ripara record di avvio | Scarica strumento di riparazione**

Opzioni di azione in caso di rilevamento di record di avvio infetto: in caso di drive del floppy disk infetti sono disponibili opzioni per effettuare la riparazione. Se con il programma AntiVir non è possibile effettuare alcuna riparazione, è possibile scaricare uno strumento speciale che riconosce e rimuove i virus del record di avvio.

Suggerimenti
Se si applicano azioni su processi in corso, i processi interessati vengono terminati prima dell'esecuzione dell'azione.

Azioni di Guard in caso di file rilevati dal componente ProActiv (messaggio di azioni sospette di un'applicazione):

– **Programma attendibile**

L'esecuzione dell'applicazione prosegue. Il programma viene inserito nell'elenco delle applicazioni consentite ed escluso dal monitoraggio mediante il componente ProActiv. Aggiungendolo nell'elenco delle applicazioni consentite viene impostato il tipo di monitoraggio *Contenuti*. Questo significa che l'applicazione viene esclusa dal monitoraggio mediante il componente ProActiv solo in caso di contenuti non modificati (vedere Configurazione::Guard::ProActiv::Filtro delle applicazioni: Applicazioni consentite).

– **Blocca il programma una volta**

L'applicazione viene bloccata, quindi l'esecuzione dell'applicazione viene terminata. Le azioni dell'applicazione continuano a essere monitorate dal componente ProActiv.

– **Blocca sempre questo programma**

L'applicazione viene bloccata, quindi l'esecuzione dell'applicazione viene terminata. Il programma viene inserito nell'elenco delle applicazioni da bloccare e non può più essere eseguito (vedere Configurazione::Guard::ProActiv::Filtro delle applicazioni: Applicazioni da bloccare).

– **Ignora**

L'esecuzione dell'applicazione prosegue. Le azioni dell'applicazione continuano a essere monitorate dal componente ProActiv.

Azioni di MailGuard: Email in ingresso

– **Sposta in quarantena**

L'email viene spostata in Quarantena unitamente agli allegati. L'email infetta viene eliminata. Il corpo del testo e gli allegati delle email vengono sostituiti da un testo standard.

– **Elimina**

L'email infetta viene eliminata. Il corpo del testo e gli allegati delle email vengono sostituiti da un testo standard.

– **Elimina allegato**

L'allegato infetto viene sostituito da un testo standard. Se il corpo del testo dell'email risulta infetto, viene eliminato ed eventualmente sostituito da un testo standard. L'email stessa viene inoltrata.

– **Sposta allegato in quarantena**

L'allegato infetto viene collocato in Quarantena e infine eliminato (sostituito da un testo standard). Il corpo dell'email viene inoltrato. L'allegato infetto potrà essere successivamente inoltrato con il Gestore della quarantena.

– **Ignora**

L'email infetta viene inoltrata.

Attenzione
In questo modo virus e programmi indesiderati potrebbero accedere al computer. Selezionare l'opzione **Ignora** solo in casi eccezionali. Disattivare l'anteprima in Microsoft Outlook, non aprire mai gli allegati facendo doppio clic!

Azioni di MailGuard: Email in uscita

– **Sposta email in quarantena (non inviare)**

L'email unitamente agli allegati viene copiata in Quarantena e non inviata. L'email resta nella Posta in uscita del client email. Nel programma email viene visualizzato un messaggio di errore. In tutte le procedure di invio seguenti dell'account di posta elettronica questo messaggio viene verificato per malware.

– **Blocca invio email (non inviare)**

L'email non viene inviata e resta nella Posta in uscita del client email. Nel programma email viene visualizzato un messaggio di errore. In tutte le procedure di invio seguenti dell'account di posta elettronica questo messaggio viene verificato per malware.

– **Ignora**

Le email infette vengono inviate.

Attenzione
In questo modo virus e programmi indesiderati potrebbero raggiungere il computer del destinatario dell'email.

Azioni di WebGuard:

– **Nega accesso**

Il sito Web richiesto dal server Web o i dati e i file trasferiti non vengono inviati al proprio browser Web. Nel browser Web viene visualizzato un messaggio di errore relativo al divieto di accesso.

– **Sposta in quarantena**

Il sito web richiesto dal server web o i dati e i file trasferiti non vengono spostati nella quarantena. Il file infetto può essere ripristinato dal Gestore della quarantena se ha un valore informativo, oppure, se necessario, inviato ad Avira Malware Research Center.

– **Ignora**

Il sito Web richiesto dal server Web o i dati e i file trasferiti vengono inoltrati da WebGuard al proprio browser Web.

Attenzione
In questo modo virus e programmi indesiderati potrebbero accedere al computer. Selezionare l'opzione **Ignora** solo in casi eccezionali.

Suggerimenti
Consigliamo di spostare in quarantena un file sospetto che non può essere riparato.

Suggerimenti
Inviare a noi i file da analizzare che sono stati segnalati dall'euristica.
É possibile caricare i file ad esempio dal nostro sito web:http://www.avira.it/file-upload
I file segnalati dall'euristica si riconoscono dalla definizione *HEUR/* o *HEURISTIC/*, che viene anteposta al nome del file, ad esempio: *HEUR/provafile.**.

5.2.10 Quarantena: Trattare file (*.qua) in quarantena

É possibile trattare i file in quarantena nel modo seguente:

- In Control Center selezionare la rubrica **Gestione :: Quarantena**.
- Verificare di quali file si tratta cosicché sia possibile ripristinare gli originali sul computer.

Se si desidera visualizzare maggiori informazioni su un file:

- Selezionare il file e fare clic su .

→ Apparirà la finestra di dialogo *Proprietà* con ulteriori informazioni sul file.

Se si desidera verificare nuovamente un file:

La verifica di un file è consigliata quando il file di definizione dei virus del programma AntiVir è stato aggiornato ed esiste il sospetto di un falso allarme. É così possibile confermare un falso allarme a una successiva verifica e ripristinare il file.

- Selezionare il file e fare clic su .

→ Il file viene controllato utilizzando le impostazioni della scansione diretta per virus e malware.

→ Dopo il controllo appare la finestra di dialogo *Statistiche della scansione* che visualizza la statistica relativa allo stato del file prima e dopo la nuova scansione.

Se si desidera eliminare un file:

- Selezionare il file e fare clic su .

Se si desidera caricare il file da analizzare su un server Web di Avira Malware Research Center:

- Selezionare il file che si desidera caricare.
- Fare clic su .

→ Si aprirà una finestra di dialogo con un modulo per inserire i dati personali a cui essere contattati.

- Indicare per intero i propri dati.

- Selezionare un tipo: **File sospetto** o **Falso allarme**.
- Premere su **OK.**

→ Il file compresso viene caricato su un server Web di Avira Malware Research Center.

Suggerimenti
Nei seguenti casi si consiglia un'analisi da parte di Avira Malware Research Center:
Oggetto euristico (file sospetto): Durante una scansione un file del programma AntiVir è stato identificato come sospetto e spostato in quarantena: Nella finestra di dialogo per il rilevamento di virus o nel file di report della scansione è stata consigliata l'analisi del file da parte di Avira Malware Research Center.
File sospetto: Il file ritenuto sospetto è stato aggiunto alla quarantena, tuttavia la verifica del file per virus e malware ha dato esito negativo.
Falso allarme: Si parte dal presupposto che si tratti di un falso allarme nel rilevamento di un virus: Il programma AntiVir indica un rilevamento in un file che tuttavia con tutta probabilità non è infetto da malware.

Suggerimenti
La dimensione dei file caricati si limita a 20 MB non compressi o a 8 MB compressi.

Suggerimenti
È possibile caricare solo un singolo file.

Se si desidera copiare un oggetto in quarantena in un altra directory:

- Selezionare il file in quarantena e fare clic su .

→ Si apre una finestra di dialogo in cui è possibile selezionare una directory.

- Selezionare una directory nella quale deve essere archiviata una copia dell'oggetto in quarantena e confermare.

→ L'oggetto in quarantena selezionato viene archiviato nella directory scelta.

Suggerimenti
L'oggetto in quarantena non è uguale al file ripristinato. L'oggetto in quarantena è crittografato e non può essere eseguito o letto nel formato originale.

Se si desidera esportare in un file di testo le proprietà di un oggetto in quarantena selezionato:

- Selezionare il file in quarantena e fare clic su .

→ Si apre un file di testo con i dati dell'oggetto in quarantena scelto.

- Salvare il file di testo.

I file in quarantena possono anche essere ripristinati:

– vedere capitolo: Quarantena: Ripristina file in quarantena

5.2.11 Quarantena: Ripristina file in quarantena

In base al sistema operativo sono disponibili diversi sistemi per il ripristino:

– In Windows XP e 2000:

 Con questo simbolo si ripristinano i file nella directory originale.

Con questo simbolo si ripristinano i file nella directory selezionata.

– In Windows Vista:

In Microsoft Windows Vista il Control Center ha inizialmente diritti limitati ad esempio per l'accesso a file e directory. Alcune azioni e l'accesso ai file possono essere eseguiti dal Control Center solo con diritti di amministratore avanzati. Questi diritti di amministratore avanzati devono essere assegnati a ogni avvio di una scansione mediante un profilo di scansione.

 Con questo simbolo si ripristinano i file nella directory selezionata.

Con questo simbolo si ripristinano i file nella directory originale. Se per l'accesso a questa directory sono necessari diritti di amministratore avanzati, appare una richiesta corrispondente.

É possibile ripristinare i file in quarantena nel modo seguente:

Attenzione
Pericolo di perdita di dati e danni al sistema operativo del computer! Utilizzare la funzione *Ripristina l'oggetto selezionato* solo in casi eccezionali. Ripristinare solo quei file che possono essere riparati con una nuova scansione.

✓ File nuovamente controllato e riparato con una scansione.

▶ In Control Center selezionare la rubrica **Gestione :: Quarantena**.

Suggerimenti

È possibile ripristinare email e allegati di email solo con l'opzione e con l'estensione **.eml*.

Se si desidera ripristinare un file nella sua posizione originale:

▶ Evidenziare il file e fare clic sul simbolo (Windows 2000/XP: , Windows Vista).

Questa opzione non è disponibile per le email.

Suggerimenti

È possibile ripristinare email e allegati di email solo con l'opzione e con l'estensione **.eml*.

→ Viene richiesto quindi se si desidera ripristinare il file.

▶ Fare clic su **Sì**.

→ Il file viene ripristinato nella directory dalla quale è stato spostato in quarantena.

Se si desidera ripristinare un file in una determinata directory:

▶ Selezionare il file e fare clic su .

→ Viene richiesto quindi se si desidera ripristinare il file.

▶ Fare clic su **Sì**.

→ Apparirà la finestra standard di Windows per la selezione di una directory.

▶ Selezionare la directory nella quale si desidera ripristinare il file e confermare.

→ Il file viene ripristinato nella directory selezionata.

5.2.12 Quarantena: Sposta i file sospetti in quarantena

É possibile spostare in quarantena i file sospetti manualmente come segue:

- In Control Center selezionare la rubrica **Gestione :: Quarantena**.
- Fare clic su .

→ Apparirà la finestra standard di Windows per la selezione di un file.

- Selezionare il file e confermare.

→ Il file viene spostato in quarantena.

É possibile controllare i file in quarantena con AntiVir Scanner:

- vedere capitolo: Quarantena: Trattare file (*.qua) in quarantena

5.2.13 Profilo di ricerca: Inserisci o elimina un tipo di file in un profilo di ricerca

Per stabilire per un profilo di ricerca i tipi di file da scansionare o i tipi di file che devono essere esclusi dalla ricerca (possibile solo con selezione manuale e profili di ricerca personalizzati):

✓ In Control Center, nella rubrica **Protezione locale ::** *Verifica*.

- fare clic con il tasto destro del mouse sul profilo di ricerca che si desidera modificare.

→ Apparirà un menu contestuale.

- Selezionare la voce **Filtro file**.
- Aprire nuovamente il menu contestuale facendo clic sul piccolo triangolo sul lato destro del menu contestuale.

→ Appariranno le voci *Standard*, *Controlla tutti i file* e *Personalizzato*.

- Selezionare la voce **Personalizzato**.

→ Apparirà la finestra di dialogo *Estensione file* con un elenco di tutti i tipi di file che devono essere abbinati al profilo di ricerca.

Se si desidera escludere un tipo di file dalla scansione:

- Selezionare il tipo di file e fare clic su **Elimina**.

Se si desidera aggiungere un tipo di file dalla scansione:

- Selezionare il tipo di file.
- Fare clic su **Aggiungi** e inserire l'estensione del tipo di file nel campo.

  Utilizzare un massimo di 10 caratteri e non inserire punti. I metacaratteri (* e ?) sostitutivi sono consentiti.

5.2.14 Profilo di ricerca: Creare un collegamento sul desktop per il profilo di ricerca

Mediante un collegamento sul desktop per un profilo di ricerca è possibile avviare una scansione diretta facendo clic sul desktop senza richiamare il Control Center di AntiVir.

É possibile creare un collegamento al profilo di ricerca dal desktop:

✓ In Control Center, nella rubrica **Protezione locale ::** *Verifica*.

▶ selezionare il profilo di ricerca di cui si intende creare il collegamento.

▶ Fare clic sul simbolo .

→ Viene creato un collegamento sul desktop.

5.2.15 Eventi: Filtrare eventi

In Control Center sotto **Panoramica :: Eventi**, vengono visualizzati eventi creati dai componenti del programma AntiVir (analogamente al visualizzatore eventi del sistema operativo di Windows). Le componenti del programma sono:

- Updater
- Guard
- MailGuard
- Sistema di scansione
- Scheduler
- FireWall
- WebGuard
- Backup
- Servizio di assistenza
- ProActiv

Vengono visualizzati i seguenti tipi di eventi:

- Informazioni
- Attenzione
- Errore
- Rilevamento

Come filtrare gli eventi visualizzati:

▶ In Control Center selezionare la rubrica **Panoramica :: Eventi**.

▶ Attivare la casella delle componenti di programma per visualizzare gli eventi delle componenti attive.

- OPPURE -

Disattivare la casella di spunta dei componenti di programma per non visualizzare gli eventi dei componenti disattivati.

▶ Attivare la casella dei tipi di evento per visualizzare questi eventi.

- OPPURE -

Disattivare la casella di spunta dei tipi di evento per non visualizzare questi eventi.

5.2.16 MailGuard: Escludere indirizzi email dalla scansione

È possibile impostare come segue quali indirizzi email (mittente) devono essere esclusi dal controllo di MailGuard (cosiddetta white list):

▶ Selezionare la rubrica **Protezione Online :: nel Control Center. MailGuard**.

→ Nell'elenco vengono visualizzate le email in ingresso.

▶ Selezionare l'email che si desidera escludere dal controllo di MailGuard.

▶ Fare clic sul simbolo desiderato per escludere le email dal controllo di MailGuard:

L'indirizzo email selezionato non verrà più verificato per virus e programmi indesiderati.

L'indirizzo email selezionato non verrà più verificato per lo spam.

→ L'indirizzo email del mittente verrà inserito nell'elenco delle eccezioni e non verrà più verificato per virus, malware o spam.

Attenzione
Escludere solo indirizzi email di mittenti assolutamente affidabili dal controllo di MailGuard.

Suggerimenti
Nella configurazione in MailGuard :: Generale :: Eccezioni è possibile inserire altri indirizzi email o eliminarne alcuni.

5.2.17 MailGuard: Configurare il modulo AntiSpam

Il modulo AntiSpam contiene una banca dati di configurazione. In questa banca dati vengono inseriti i criteri di categorizzazione definiti dall'utente. Nel corso del tempo si impostano quindi i filtri interni, gli algoritmi e i criteri di valutazione per lo spam in base ai propri criteri personali.

É possibile categorizzare le email per la banca dati come segue:

▶ Selezionare la rubrica **Protezione Online :: nel Control Center. MailGuard**.

→ Nell'elenco è possibile vedere le email in entrata.

▶ Selezionare le email che si desidera categorizzare.

▶ Fare clic sul simbolo desiderato ad esempio per contrassegnare le email come spam o come desiderate, ovvero come "buone" .

→ L'email viene inserita nella banca dati training e verrà utilizzata la volta successiva per il riconoscimento di spam.

Suggerimenti
É possibile eliminare la banca dati training nella configurazione in MailGuard :: Generale :: Elimina AntiSpam.

5.2.18 FireWall: Selezionare il livello di sicurezza per il FireWall

É possibile scegliere tra diversi livelli di sicurezza. In base ad esse si ha la possibilità di scegliere diverse possibilità di configurazione per le regole adattatore.

Sono disponibili i seguenti livelli di sicurezza:

- **Basso**
- Il flooding e il Port-Scan vengono riconosciuti.
- **Medio**
- I pacchetti TCP e UDP sospetti vengono respinti.
- Vengono impediti il flooding e il Port-Scan.
- **Elevato**
- Il computer non è visibile sulla rete.
- I collegamenti dall'esterno vengono bloccati.
- Vengono impediti il flooding e il Port-Scan.
- **Utente**
- Regole personalizzate: con questo livello di sicurezza il programma è automaticamente convertito se sono state modificate le regole adattatore.

Suggerimenti
L'impostazione standard del livello di sicurezza per tutte le regole predefinite del FireWall di Avira è **elevato**.

É possibile impostare il livello di sicurezza del FireWall come segue:

▶ Selezionare la rubrica Protezione **Online :: nel Control Center. FireWall**.

▶ Impostare il cursore di riempimento sul livello di sicurezza desiderato.

→ Il livello di sicurezza scelto è attivo subito dopo la selezione.

5.2.19 Backup: Creazione manuale di backup

Lo strumento Backup in Control Center consente di creare in modo semplice e rapido un backup dei dati personali. Backup di Avira consente di creare i cosiddetti backup speculari, con i quali è possibile eseguire il backup dei dati e mettere a disposizione i dati più aggiornati risparmiando risorse. Durante la memorizzazione con Backup di Avira è possibile verificare i dati da mettere al sicuro da virus e malware. I file infetti non vengono salvati.

Suggerimenti
Nei backup speculari, a differenza di quelli delle versioni, non vengono mantenute singole versioni del backup. Il backup speculare contiene lo stato dei dati al momento dell'ultimo backup. Se nel gruppo dei dati da sottoporre a backup vengono eliminati dei file, non avviene alcun confronto in occasione del backup successivo, ovvero i file eliminati sono ancora presenti nel backup.

Suggerimenti
Per impostazione predefinita Il Backup di Avira effettua il backup dei soli dati modificati ed effettua un controllo sulla presenza di virus e malware. Queste impostazioni si possono modificare nella configurazione in Backup::Impostazioni.

Per memorizzare i dati con lo strumento backup:

- In Control Center selezionare la rubrica **Strumenti:: Backup**.

→ Vengono visualizzati i profili di backup predefiniti.

- Selezionare un profilo di backup predefinito.

  - OPPURE -

- Adeguare il profilo *Selezione manuale*.

  - OPPURE -

- Creare un nuovo profilo di backup
- Nel campo *Directory di destinazione* immettere una destinazione di memorizzazione per il profilo selezionato.

  Come destinazione di memorizzazione per il backup è possibile selezionare una directory sul computer o su un drive di rete collegato nonché un supporto dati rimovibile, come una penna USB o un floppy disk.

- Fare clic sul simbolo .

→ Viene visualizzata la finestra *Backup di Avira* e il backup si avvia. Lo stato e gli eventi del backup vengono visualizzati nella finestra di backup.

Se si desidera adeguare un profilo di backup:

- Aprire in *Selezione manuale* la struttura dei file fin quando non vengono aperti tutti i drive e le directory che devono essere memorizzati:
  - Fare clic sul segno +: viene visualizzato il livello della directory.
  - Fare clic sul segno -: viene nascosto il livello della directory.
- Selezionare i nodi e le directory da memorizzare facendo clic sulla casella di controllo corrispondente al livello directory desiderato:

  Si hanno le seguenti possibilità per selezionare le directory:
  - Directory incluse le sottodirectory (segno di spunta nero)
  - Directory escluse le sottodirectory (segno di spunta verde)
  - Solo le sottodirectory in una directory (segno di spunta grigio, le sottodirectory hanno un segno di spunta nero)
  - Nessuna directory (nessun segno di spunta)

Se si desidera creare un nuovo profilo di backup:

- Fare clic sul simbolo **Crea nuovo profilo**.

→ Il *Nuovo profilo* appare tra quelli già esistenti.

- Rinominare eventualmente il profilo di backup facendo clic sul simbolo .
- Selezionare i nodi e le directory da memorizzare facendo clic sulla casella di controllo in ciascun livello directory.

  Si hanno le seguenti possibilità per selezionare le directory:
  - Directory incluse le sottodirectory (segno di spunta nero)

– Directory escluse le sottodirectory (segno di spunta verde)
– Solo le sottodirectory in una directory (segno di spunta grigio, le sottodirectory hanno un segno di spunta nero)
– Nessuna directory (nessun segno di spunta)

5.2.20 Backup: Creazione di backup automatizzati

In questo modo si definisce un job che consente di creare backup automatizzati:

▶ Selezionare in Control Center la rubrica **Gestione::Scheduler**.

▶ Fare clic sul simbolo .

➔ Appare la finestra di dialogo *Nome e descrizione del job*.

▶ Assegnare un nome al job e descriverlo.

▶ Fare clic su **Avanti**.

➔ Appare la finestra di dialogo *Tipo di job*.

▶ Selezionare **Job di backup**.

▶ Fare clic su **Avanti**.

➔ Appare la finestra di dialogo *Selezione del profilo*.

▶ Selezionare quale profilo deve essere scansionato.

Suggerimenti
Viene visualizzato esclusivamente il profilo di backup per il quale è stata immessa una destinazione di memorizzazione.

▶ Fare clic su **Avanti**.

➔ Apparirà la finestra di dialogo *Durata del job*.

▶ Selezionare quando deve essere eseguita la scansione:

– **Immediato**
– **Giornaliero**
– **Settimanale**
– **Intervallo**
– **Unico**
– **Login**
– **Plug&Play**

Per l'evento Plug&Play viene sempre creato un backup quando il supporto dati rimovibile selezionato come destinazione di memorizzazione per il profilo di backup viene collegato al computer. Per questo evento, Plug&Play, è necessario avere definito una chiavetta USB come destinazione di memorizzazione.

▶ Indicare il termine in base alla selezione.

▶ Selezionare una delle seguenti opzioni aggiuntive (disponibili in base al tipo di job):

– **Ripeti job se il tempo è già scaduto**

Vengono eseguiti job scaduti che non è stato possibile eseguire al momento designato, ad esempio perché il computer era spento.

▶ Fare clic su **Avanti**.

→ Appare la finestra di dialogo *Selezione della modalità di visualizzazione*.

▶ Selezionare la modalità di visualizzazione della finestra del job:

- **Ridotta**: solo la barra di progressione
- **Estesa**: l'intera finestra di backup
- **Invisibile**: nessuna finestra di backup

▶ Fare clic su **Fine**.

→ Il nuovo job assegnato viene visualizzato alla pagina iniziale della rubrica *Gestione :: Scheduler* come attivato (segno di spunta).

▶ Disattivare i job che non devono essere eseguiti.

Mediante i seguenti simboli, è possibile elaborare ulteriormente i job:

 Visualizza proprietà di un job

 Modifica job

 Elimina job

 Avvia job

 Arresta job

6 Sistema di scansione

Con il componente Scanner è possibile effettuare scansioni mirate per virus e programmi indesiderati (scansione diretta). È possibile effettuare una scansione per file infetti in diversi modi:

- **Scansione diretta mediante menu contestuale**
  La scansione diretta mediante il menu contestuale (tasto destro del mouse - voce **Controlla i file selezionati con AntiVir**) si consiglia quando, ad esempio, si desidera controllare singoli file e directory in Esplora risorse di Windows. Un ulteriore vantaggio è che il Control Center non deve essere avviato per la scansione diretta mediante il menu contestuale.
- **Scansione diretta con Drag & Drop**
  Trascinando un file o una directory nella finestra di programma del Control Center il sistema di scansione verifica il file o la directory, nonché tutte le sottodirectory. Questa procedura è consigliata quando si desidera controllare i singoli file e directory che sono stati archiviati, ad esempio, sul desktop.
- Scansione diretta per profili
  Questa procedura è consigliata quando si desidera controllare regolarmente alcune directory e drive (ad esempio la propria directory di lavoro o drive, sui quali si archiviano regolarmente nuovi file). Queste directory e drive non devono quindi essere selezionati a ogni scansione ma vengono comodamente selezionati tramite il profilo corrispondente.
- **Scansione diretta con Scheduler**
  offre la possibilità di far eseguire job temporizzati di scansione.

Durante la scansione per rootkit, virus del record di avvio e durante la scansione dei processi attivi sono necessari dei procedimenti particolari. Sono disponibili le seguenti opzioni:

- Scansione di rootkit mediante il profilo di ricerca *Scansiona rootkit*
- Scansione dei processi attivi mediante il profilo di ricerca **Processi attivi**
- Scansiona virus del record di avvio con il comando **Scansiona virus del record di avvio** nel menu **Extra**

7 Aggiornamenti

L'efficacia di un software antivirus dipende dall'aggiornamento del programma, in particolare del file di definizione dei virus e del motore di ricerca. Per l'esecuzione degli aggiornamenti, il componente Updater è integrato in AntiVir . Updater garantisce che il programma AntiVir sia sempre il più aggiornato possibile e che sia in grado di rilevare i nuovi virus che compaiono quotidianamente. Updater aggiorna i seguenti componenti:

– File di definizione dei virus:

  Il file di definizione dei virus contiene il modello di rilevamento del programma dannoso che il programma AntiVir utilizza nella scansione per virus e malware nonché nella riparazione di oggetti infetti.

– Motore di ricerca:

  Il motore di ricerca contiene i metodi che vengono utilizzati dal programma AntiVir per la scansione per virus e malware.

– File di programma (aggiornamento del prodotto):

  I pacchetti di aggiornamento del prodotto mettono a disposizione ulteriori funzioni per i singoli componenti del programma.

Durante un aggiornamento viene verificato lo stato di aggiornamento del file di definizione dei virus e del motore di ricerca e, se necessario, tali componenti vengono aggiornati. In base alle impostazioni di configurazione Updater esegue un aggiornamento del prodotto o segnala la disponibilità di tale aggiornamento. Terminato un aggiornamento del prodotto può essere necessario riavviare il sistema. Se l'aggiornamento avviene solo per il file di definizione dei virus e del motore di ricerca non è necessario riavviare il computer.

Suggerimenti
Per motivi di sicurezza, l'Updater verifica se il file host di Windows del computer è stato modificato, ad esempio con manipolazione da parte di malware dell'URL di aggiornamento, a seguito della quale l'Updater viene indirizzato su pagine di download indesiderate. Se il file host di Windows è stato manipolato, l'evento viene riportato nel file di report di Updater.

Un aggiornamento viene eseguito in automatico nel seguente intervallo: 2 Ore. È possibile modificare o disattivare l'aggiornamento automatico dalla configurazione (Configurazione::Aggiorna).

In Control Center in è possibile configurare ulteriori job di aggiornamento che Updater deve eseguire a intervalli definiti. È inoltre possibile avviare l'aggiornamento manualmente:

– In Control Center: nel menu Aggiornamento e della rubrica Stato
– Tramite il menu contestuale dell'icona Tray

Gli aggiornamenti vengono richiamati da Internet tramite un server Web del produttore. Normalmente si utilizza la connessione di rete esistente per collegarsi al server di download di Avira GmbH. Questa impostazione standard può essere modificata nella configurazione in Generale :: Aggiornamento.

8 Avira FireWall :: Panoramica

Avira FireWall monitora e regola il traffico dati in entrata e in uscita sul computer e lo protegge dai numerosi attacchi e minacce provenienti da Internet: in base alle direttive di sicurezza, il traffico dati in entrata e in uscita o l'attesa delle porte vengono consentiti o rifiutati. Quando Avira FireWall rifiuta le attività di rete bloccando così le connessioni Internet, si riceve un messaggio sul desktop. Sono disponibili le seguenti possibilità di impostazione di Avira FireWall:

– mediante l'impostazione di un livello di sicurezza nel Control Center

In Control Center è possibile impostare un livello di sicurezza. I livelli di sicurezza *Basso*, *Medio* e *Alto* contengono ognuno più regole di sicurezza integrative basate su filtri di pacchetto. Queste regole di sicurezza vengono memorizzate come regole adattatore predefinite in FireWall::Regole adattatore.

– memorizzando le azioni nella finestra Evento di rete

Se un'applicazione tenta per la prima volta di creare una connessione alla rete o a Internet, si apre la finestra pop up *Evento di rete*. Nella finestra *Evento di rete*, l'utente può scegliere se l'attività di rete dell'applicazione viene consentita o rifiutata. Se l'opzione **Memorizza azione per questa applicazione** è attivata, l'azione viene creata come regola di applicazione e memorizzata nella configurazione sotto FireWall::Regole di applicazione. Memorizzando le azioni nella finestra Evento di rete, si ottiene un set di regole per le attività di rete delle applicazioni.

Suggerimenti
In caso di applicazioni di fornitori affidabili, l'accesso alla rete viene consentito per default purché una regola adattatore non vieti l'accesso alla rete. È possibile rimuovere fornitori dall'elenco dei fornitori affidabili.

– mediante la creazione di regole adattatore e di applicazione in Configurazione

Nella configurazione è possibile modificare le regole adattatore predefinite o crearne di nuove. Se si aggiungono o modificano le regole adattatore il livello di sicurezza del FireWall viene impostato automaticamente sul valore *Utente*.
Con le regole adattatore è possibile definire regole di monitoraggio specifiche per le applicazioni:
Con semplici regole di applicazione, è possibile impostare se tutte le attività di rete di un'applicazione software debbano essere rifiutate o consentite o vadano trattate in modo interattivo tramite la finestra di pop up *Evento di rete*.
Nella configurazione estesa della rubrica *Regole di applicazione*, è possibile definire per un'applicazione diversi filtri di pacchetto che vengono eseguiti come regole di applicazione specifiche.

Suggerimenti
Per le regole di applicazione si distinguono due modalità: *privilegiata* e *filtrata*. Per le regole di applicazione in modalità *filtrata*, viene data priorità alle regole adattatore appropriate; ciò significa che la regola adattatore più adatta viene eseguita dopo la regola di applicazione. Quindi può accadere che l'accesso di rete da parte di applicazioni consentite venga rifiutato a causa di un livello di sicurezza alto o in base alle rispettive regole adattatore. In caso di regole di applicazione in modalità *privilegiata* le regole adattatore vengono ignorate. Se le applicazioni vengono consentite in modalità *privilegiata*, l'accesso alla rete da parte dell'applicazione viene comunque consentito.

9 Backup

Sono disponibili varie opzioni per creare un backup dei dati:

Backup tramite lo strumento di backup

Grazie agli strumenti di backup è possibile selezionare o creare un profilo di backup e avviare manualmente un backup per un profilo selezionato.

Backup tramite un job di backup in

Lo offre la possibilità di creare job di backup temporizzati o attivati da eventi. I job di backup vengono eseguiti automaticamente dallo . Questa procedura è l'ideale se di desidera salvare regolarmente dati specifici.

10 Risoluzione di problemi, suggerimenti

In questo capitolo In questo capitolo sono presenti indicazioni importanti per la risoluzione di problemi e ulteriori suggerimenti inerenti al programma AntiVir acquistato.

Vedere capitolo Assistenza in caso di problemi

Vedere capitolo Shortcut

vedi capitolo Centro sicurezza Windows

10.1 Assistenza in caso di problemi

Qui sono reperibili informazioni sulle cause e le soluzioni di eventuali problemi.

- Viene visualizzato il messaggio di errore *Il file di licenza non si apre*.
- AntiVir MailGuard non funziona.
- Non è possibile effettuare connessioni a Internet in macchine virtuali se Avira FireWall è installato sul sistema operativo host e il livello di sicurezza di Avira FireWall è impostato su Medio o Elevato.
- La connessione Virtual Private Network (VPN) è bloccata se il livello di sicurezza di Avira FireWall è impostato su Medio o Elevato.
- Un'email inviata mediante una connessione TSL, è stata bloccata da MailGuard.
- Webchat non funziona: non vengono visualizzati i messaggi chat

Viene visualizzato il messaggio di errore *Il file di licenza non si apre*.

Causa: il file è protetto.

▶ Per attivare la licenza non bisogna aprire il file, ma salvarlo nella directory del programma.

Il messaggio di errore *Lo stabilimento della connessione è fallito durante il download del file ...* appare nel tentativo di avviare un aggiornamento.

Causa: la connessione Internet non è attiva. Pertanto, non può essere creato alcun collegamento al server Web in Internet.

▶ Provare se altri servizi Internet come WWW o l'email funzionano. Se non funzionano ripristinare la connessione Internet.

Causa: il server proxy non è raggiungibile.

▶ Verificare se sia cambiato il login per il server proxy e adattare eventualmente la propria configurazione.

Causa: il file update.exe non è ammesso dal proprio firewall.

▶ Assicurarsi che il file update.exe sia ammesso dal proprio firewall.

Altrimenti:

▶ Verificare la propria configurazione (Modalità esperto) in Generale :: Aggiornamento.

Impossibile spostare o eliminare virus e malware.

Causa: il file è stato caricato da Windows ed è attivo.

- Aggiornare il prodotto AntiVir.
- Se si utilizza il sistema operativo Windows XP, disattivare il ripristino del sistema.
- Avviare il computer in modalità provvisoria.
- Avviare il programma AntiVir e la configurazione (Modalità esperto).
- Selezionare Sistema di scansione :: Scansione :: File :: Tutti i file e confermare con **OK**.
- Avviare una scansione su tutti i drive locali.
- Avviare il computer in modalità normale.
- Eseguire una scansione in modalità normale.
- Se non vengono rilevati altri virus e malware attivare il ripristino del sistema se è disponibile e deve essere utilizzato.

L'icona Tray mostra uno stato disattivato.

Causa: AntiVir Guard è disattivato.

- fare clic in Control Center nella rubrica Panoramica :: Stato nella sezione AntiVir Guard sul link **Attiva**.

Causa: AntiVir Guard è bloccato da un firewall.

- Nella configurazione del firewall definire un permesso generale per AntiVir Guard. AntiVir Guard lavora esclusivamente con l'indirizzo 127.0.0.1 (localhost). Non viene stabilita alcuna connessione Internet. Lo stesso vale per AntiVir MailGuard.

Altrimenti:

- Verificare la modalità di attivazione del servizio AntiVir Guard. Attiva eventualmente il servizio: selezionare in "Start | Impostazioni | Pannello di controllo". Avviare il pannello di configurazione "Servizi" facendo doppio clic (in Windows 2000 e Windows XP l'applet servizi si trova nella sottodirectory "Gestione"). Cercare la voce *Avira AntiVir Guard*. Come modalità di avviamento deve essere inserito "Automatico" e come stato "Avviato". Avviare il servizio manualmente mediante la selezione della riga corrispondente e del pulsante "Avvia". Se viene visualizzato un messaggio di errore, verificare la visualizzazione eventi.

Il computer diventa estremamente lento se eseguo un backup.

Causa: AntiVir Guard scansiona tutti i dati con i quali lavora il backup durante il processo di backup.

- Selezionare nella configurazione (Modalità esperto) Guard :: Scansione :: Eccezione e inserire il nome del processo del software di backup.

Il mio firewall segnala AntiVir Guard e AntiVir MailGuard, se sono attivi.

Causa: la comunicazione di AntiVir Guard e AntiVir MailGuard avviene mediante il protocollo Internet TCP/IP. Un firewall monitora tutte le connessioni mediante questo protocollo.

- Definire un permesso generale per AntiVir Guard e AntiVir MailGuard. AntiVir Guard lavora esclusivamente con l'indirizzo 127.0.0.1 (localhost). Non viene stabilita alcuna connessione Internet. Lo stesso vale per AntiVir MailGuard.

AntiVir MailGuard non funziona.

Verificare la funzionalità di AntiVir MailGuard sulla base delle seguenti checklist se si manifestano problemi con AntiVir MailGuard.

Checklist

- Verificare se il client mail si registra mediante Kerberos, APOP o RPA sul server. Questi metodi di autenticazione attualmente non vengono supportati.
- Verificare se il client mail viene registrato mediante SSL (spesso chiamato anche TSL - Transport Layer Security) sul server. AntiVir MailGuard non supporta alcun SSL e chiude pertanto le connessioni SSL crittografate. Se si desidera utilizzare le connessioni SSL crittografate senza la protezione di MailGuard, per la connessione occorre usare una porta diversa da quelle controllate da MailGuard. Le porte monitorate da MailGuard possono essere configurate nella configurazione in MailGuard::Scansione.
- Il servizio AntiVir MailGuard è attivo? Attiva eventualmente il servizio: selezionare in "Start | Impostazioni | Pannello di controllo". Avviare il pannello di configurazione "Servizi" facendo doppio clic (in Windows 2000 e Windows XP l'applet servizi si trova nella sottodirectory "Gestione"). Cercare la voce *Avira AntiVir MailGuard*. Come modalità di avviamento deve essere inserito "Automatico" e come stato "Avviato". Avviare il servizio manualmente mediante la selezione della riga corrispondente e del pulsante "Avvia". Se viene visualizzato un messaggio di errore, verificare la visualizzazione eventi. Se non riesce, disinstallare completamente il programma AntiVir mediante "Start | Impostazioni | Pannello di controllo | Software", riavviare il computer e, infine, installare nuovamente il programma AntiVir.

Generale

- Mediante SSL (Secure Sockets Layer) le connessioni crittografate POP3 (spesso definite anche TLS - Transport Layer Security) in questo momento non possono essere protette e vengono ignorate.
- L'autenticazione al server mail attualmente viene supportata solo con "Passwords". "Kerberos" e "RPA" attualmente non sono supportati.
- Il programma AntiVir non cerca virus o programmi indesiderati all'invio di email.

Suggerimenti
Consigliamo di eseguire regolarmente gli aggiornamenti Microsoft per colmare le eventuali lacune in termini di sicurezza.

Non è possibile effettuare connessioni a Internet in macchine virtuali se Avira FireWall è installato sul sistema operativo host e il livello di sicurezza di Avira FireWall è impostato su Medio o Elevato.

Se Avira FireWall è installato su un computer dove viene gestito un sistema virtuale (ad esempio VMWare, Virtual PC, ecc.) questo blocca tutte le connessioni di rete del sistema virtuale se il livello di sicurezza di Avira FireWall è impostato su Medio o Elevato. Se il livello di sicurezza è Basso FireWall reagisce conformemente alle aspettative.

Causa: il sistema virtuale emula una scheda di rete mediante software. Con l'emulazione i pacchetti di dati del sistema host sono incapsulati in pacchetti speciali (cosiddetti UDP) e reindirizzati mediante il gateway esterno al sistema host. In Avira FireWall vengono bloccati quelli provenienti dall'esterno a partire dal livello di sicurezza Medio.

Per gestire questo processo procedere come segue:

- Selezionare la rubrica **Protezione Online :: nel Control Center. FireWall**.
- Fare clic sul link **Configurazione**.
- Viene visualizzata la finestra di dialogo *Configurazione*. Ci si trova nella rubrica di configurazione *Regole applicazione*.
- Attivare la **Modalità esperto**.
- Selezionare la rubrica di configurazione **Regole adattatore**.
- Fare clic su **Aggiungi**.
- In *Regola in entrata* selezionare **UDP**.
- Nella sezione Nome della regola indicare un **nome**.
- Fare clic su **OK**.
- Verificare se la regola gode di un livello di priorità superiore alla regola **Rifiuta tutti i pacchetti IP**.

Attenzione
Questa regola nasconde potenziali pericoli poiché si consentono i pacchetti UDP! Dopo il funzionamento del sistema virtuale tornare al precedente livello di sicurezza.

La connessione Virtual Private Network (VPN) è bloccata se il livello di sicurezza di Avira FireWall è impostato su Medio o Elevato.

Causa: il problema è l'ultima regola della catena**Rifiuta tutti i pacchetti IP** che entra sempre in vigore quando un pacchetto non corrisponde a nessuna regola. I pacchetti inviati mediante software VPN vengono filtrati da questa regola dal momento che a causa della loro natura (cosiddetti pacchetti GRE) non ricadono in nessuna delle altre categorie.

Sostituire la regola **Rifiuta tutti i pacchetti IP** con una nuova regola che rifiuta i pacchetti TCP e UDP. In questo modo esiste la possibilità che vengano consentiti pacchetti di altri protocolli.

Un'email inviata mediante una connessione TSL, è stata bloccata da MailGuard.

Causa: Transport Layer Security (TLS: protocollo di codifica per la trasmissione dati su Internet) al momento non è supportato da MailGuard. Per inviare l'email è possibile:

- utilizzare un'altra porta rispetto alla Porta 25 impegnata da SMTP. In questo modo si aggira la sorveglianza di MailGuard
- Rinunciare alla connessione codificata TSL e disattivare il supporto TSL nel client email.
- Disattivare (ignorare) il monitoraggio delle email in uscita da parte di MailGuard nella configurazione in MailGuard::Scansione.

Webchat non funziona: i messaggi chat non vengono visualizzati, nel browser vengono caricati dei dati.

Questo fenomeno può verificarsi in chat che si basano sul protocollo HTTP con 'transfer-encoding= chunked.

Causa: WebGuard controlla i dati inviati in modo completo alla ricerca di virus e programmi indesiderati prima che i dati siano caricati nel browser Web. Durante un trasferimento di dati con "r,r;transfer-encoding= chunked" WebGuard non è in grado di rilevare la lunghezza dei messaggi o la quantità di dati.

▶ Nella configurazione impostare l'URL di Webchat come eccezione (vedere Configurazione: WebGuard::Eccezioni).

10.2 Shortcut

Le shortcut offrono la possibilità di navigare velocemente nel programma, richiamare singoli moduli e avviare azioni.

Di seguito viene presentata una panoramica delle shortcut presenti. Per maggiori informazioni sulla funzionalità e disponibilità consultare il capitolo corrispondente della guida.

10.2.1 Nelle finestre di dialogo

Shortcut	**Descrizione**
Ctrl + Tab Ctrl + Page down	Navigazione in Control Center Passa alla rubrica successiva.
Ctrl + Shift + Tab Ctrl + Page up	Navigazione in Control Center Passa alla rubrica precedente.
← ↑ → ↓	Navigazione nelle rubriche di configurazione Evidenzia con il mouse una rubrica di configurazione.
Tab	Passa all'opzione successiva o al successivo gruppo di opzioni.
Shift + Tab	Passa all'opzione precedente o al precedente gruppo di opzioni.
← ↑ → ↓	Effettua una modifica tra le opzioni di un menu a tendina selezionate o tra più opzioni in un gruppo di opzioni.
Barra spaziatrice	Attiva o disattiva una casella di controllo se l'opzione attiva è una casella di controllo.
Alt + lettera sottolineata	Seleziona l'opzione o esegui il comando.
Alt + ↓ F4	Apri il menu a tendina selezionato.
Esc	Chiudi il menu a tendina selezionato. Annulla il comando e chiudi la finestra di dialogo.

Invio	Esegui comando per l'opzione o il pulsante attivo.

10.2.2 Nella Guida in linea

Shortcut	Descrizione
Alt + barra spaziatrice	Visualizza il menu del sistema.
Alt + Tab	Passa dalla Guida in linea ad altre finestre aperte.
Alt + F4	Chiudi la Guida in linea.
Shift+ F10	Visualizza menu contestuali della Guida in linea.
Ctrl + Tab	Passa alla rubrica successiva nella finestra di navigazione.
Ctrl + Shift + Tab	Passa alla rubrica precedente nella finestra di navigazione.
Page up	Passa all'argomento che è visualizzato sopra l'argomento attuale nel sommario, nell'indice o nell'elenco dei risultati della ricerca.
Page down	Passa all'argomento che è visualizzato sotto l'argomento attuale nel sommario, nell'indice o nell'elenco dei risultati della ricerca.
Page up Page down	Sfoglia le voci su un argomento.

10.2.3 In Control Center

Generale

Shortcut	Descrizione
F1	Visualizza Guida in linea
Alt + F4	Chiudi Control Center
F5	Aggiorna visualizzazione
F8	Apri configurazione
F9	Avvia aggiornamento

Rubrica Scansiona

Shortcut	Descrizione
F2	Rinomina il profilo selezionato
F3	Avvia la scansione con il profilo selezionato

F4	Crea collegamento sul desktop per il profilo selezionato
Agg	Crea nuovo profilo
Canc	Elimina profilo selezionato

Rubrica FireWall

Shortcut	Descrizione
Invio	Proprietà

Rubrica Quarantena

Shortcut	Descrizione
F2	Riscansiona l'oggetto
F3	Ripristina l'oggetto
F4	Invia l'oggetto
F6	Ripristina l'oggetto in...
Invio	Proprietà
Agg	Aggiungi file
Canc	Elimina l'oggetto

Rubrica Scheduler

Shortcut	Descrizione
F2	Modifica job
Invio	Proprietà
Agg	Inserisci nuovo job
Canc	Elimina job

Rubrica Report

Shortcut	Descrizione
F3	Visualizza il file di report
F4	Stampa il file di report
Invio	Mostra il report
Canc	Elimina il report

Rubrica Eventi

Shortcut	Descrizione
F3	Esporta evento
Invio	Mostra evento
Canc	Elimina evento

10.3 Centro di sicurezza di Windows

- a partire da Windows XP Service Pack 2 -

10.3.1 Generale

Il Centro sicurezza di Windows verifica lo stato di un computer dal punto di vista della sicurezza.

Se viene rilevato un problema in uno di questi punti importanti (ad esempio un programma antivirus vecchio), il Centro sicurezza invia un avviso e fornisce dei suggerimenti per proteggere più efficacemente il computer.

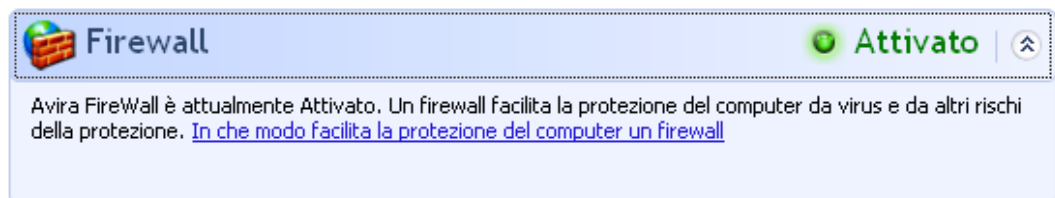
10.3.2 Il Centro sicurezza di Windows e il programma Antivir acquistato.

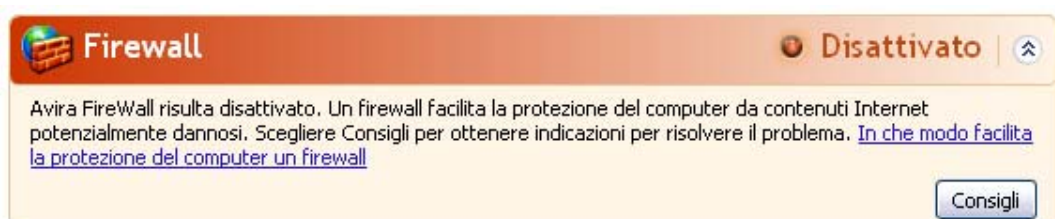
Firewall

È possibile ricevere dal Centro sicurezza le seguenti informazioni relative al firewall:

– Firewall AKTIV / Firewall attivo
– Firewall INAKTIV / Firewall non attivo

Firewall ATTIVO/Firewall non attivo

Dopo l'installazione del programma AntiVir e la chiusura del firewall di Windows si riceve il seguente avviso:

Firewall INATTIVO/Firewall non attivo

Si riceve il seguente messaggio se si disattiva il FireWall di Avira:

Suggerimenti
È possibile attivare o disattivare il FireWall di Avira tramite Stato in Control Center.

Attenzione
Se viene disattivato il FireWall di Avira, il computer non è più protetto da accessi non autorizzati dalla rete o da Internet.

Software di protezione antivirus/Protezione da software dannoso

È possibile ricevere i seguenti avvisi dal Centro sicurezza di Windows in relazione alla protezione antivirus.

Protezione antivirus NON TROVATA

Protezione antivirus NON AGGIORNATA

Protezione antivirus ATTIVA

Protezione antivirus INATTIVA

Protezione antivirus NON MONITORATA

Protezione antivirus NON TROVATA

Questo avviso del Centro sicurezza di Windows viene visualizzato quando quest'ultimo non ha rilevato alcun software antivirus sul computer.

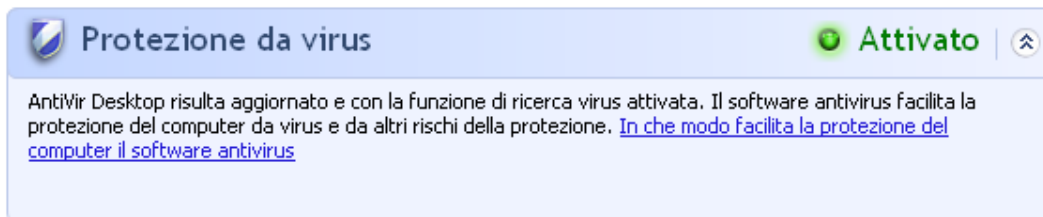
Suggerimenti
Installare il programma AntiVir sul computer per proteggerlo da virus e altri programmi indesiderati!

Protezione antivirus NON AGGIORNATA

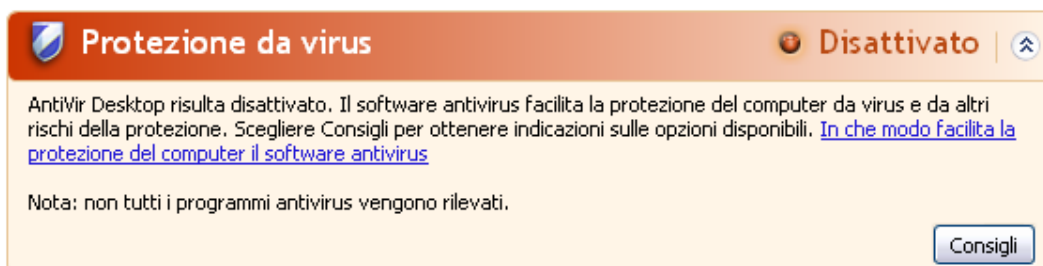
Se si possiede Windows XP Service Pack 2 o Windows Vista e si installa successivamente il programma AntiVir oppure si installa Windows XP Service Pack 2 o Windows Vista su un sistema su cui è già installato il programma AntiVir, si riceve il seguente messaggio:

Suggerimenti
Per far sì che il Centro sicurezza di Windows riconosca il programma AntiVir come aggiornato, dopo l'installazione è necessario eseguire un aggiornamento. Aggiornare il sistema eseguendo un aggiornamento.

Protezione antivirus ATTIVA

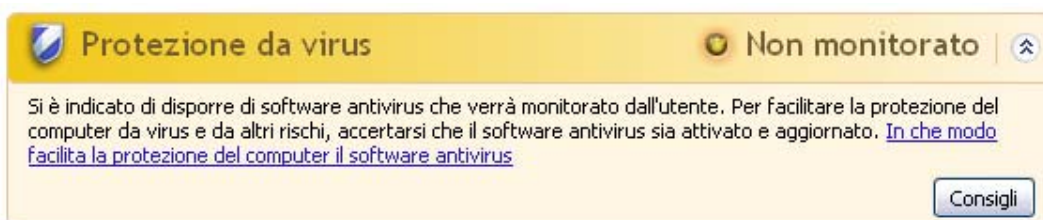
Dopo l'installazione del programma AntiVir e un susseguente aggiornamento, si riceve la seguente nota:

Il programma AntiVir è aggiornato e AntiVir Guard è attivo.

Protezione antivirus INATTIVA

Si riceve la seguente nota se si disattiva AntiVir Guard o si arresta il servizio Guard.

Note
AntiVir Guard può essere attivato o disattivato nella rubrica Panoramica :: Stato del Control Center. Inoltre AntiVir Guard viene riconosciuto come attivato quando l'ombrellino rosso nella barra delle applicazioni è aperto.

Protezione antivirus NON MONITORATA

Si riceve il seguente messaggio dal Centro sicurezza di Windows poiché si è optato per l'automonitoraggio del software antivirus.

Suggerimenti
La funzione non è supportata da Windows Vista.

Suggerimenti
Il Centro sicurezza di Windows è supportato dal programma AntiVir. È possibile attivare questa opzione in ogni momento con il pulsante "Consigli...".

Suggerimenti
Anche se sono installati Windows XP Service Pack 2 o Windows Vista, si ha comunque bisogno di una soluzione antivirus. Sebbene Windows XP Service Pack 2 controlli il software antivirus non ha alcuna funzione antivirus. L'utente non sarebbe protetto contro virus e malware senza una soluzione antivirus aggiuntiva!

11 Virus e altro

11.1 Categorie di minacce

Programmi di selezione a pagamento (DIALER)

Alcuni servizi offerti in Internet sono a pagamento. In Germania la fatturazione avviene per programmi di selezione con i numeri 0190/0900 (in Austria e Svizzera con i numeri 09x0; in Germania a medio termine passerà ai numeri 09x0). Installati sul computer, questi programmi - in breve dialer - garantiscono la creazione della connessione mediante i numeri Premium-Rate, la cui tariffa può variare enormemente.

La commercializzazione di contenuti online mediante la bolletta telefonica è legale e può essere vantaggiosa per l'utente. I dialer seri non hanno alcun dubbio sul fatto che il cliente sia consapevole e lo utilizzi in modo avveduto. Tali contenuti si installano sul computer dell'utente solo se l'utente dà la propria approvazione, espressa sulla base di un'etichettatura ben riconoscibile o di una richiesta univoca e chiara. La creazione della connessione di programmi dialer seri viene visualizzata in maniera chiara e non ambigua. Inoltre, i dialer seri informano l'utente in maniera esatta e precisa sui costi correlati.

Purtroppo però esistono dialer che si installano senza farsi notare, in maniera dubbia o addirittura fraudolenta. Sostituiscono, ad esempio, la connessione standard dial up dell'utente di Internet all'ISP (Internet-Service-Provider) e a ogni connessione selezionano numeri a pagamento spesso estremamente costosi, come i numeri 0190/0900. L'utente interessato nota dalla bolletta successiva che si è installato un programma dialer indesiderato che si connette a ogni accesso a Internet ai numeri a pagamento 0190/0900 - determinando così una bolletta estremamente cara.

Per proteggersi da programmi di selezione non desiderati e a pagamento (dialer 0190/0900), consigliamo di rivolgersi direttamente al proprio gestore telefonico per bloccare questo tipo di numeri.

Di default, il programma AntiVir riconosce i programmi di selezione a pagamento a lui noti.

Se nella configurazione di Categorie delle minacce è stata attivata l'opzione **Programmi di selezione a pagamento (DIALER)** con un segno di spunta, in caso di rilevamento di un programma di selezione a pagamento viene emesso un messaggio di avviso. Si ha quindi la possibilità di eliminare facilmente gli eventuali dialer indesiderati per i numeri 0190/0900. Se si tratta di un programma di selezione a pagamento voluto, si può dichiarare un file da escludere che non verrà più scansionato in futuro.

Giochi (GAMES)

I giochi per computer devono esistere, ma non necessariamente sul luogo di lavoro (ad eccezione a volte della pausa pranzo). Tuttavia i dipendenti delle aziende e i collaboratori degli enti pubblici spesso usano i giochi. Su Internet sono disponibili moltissimi giochi. Anche i giochi per email stanno conoscendo una rapida espansione: dai semplici scacchi fino a "battaglia navale" esistono numerose varianti: i giochi vengono inviati per email ai partner e accettati da questi ultimi.

Alcune ricerche hanno dimostrato che il tempo durante l'orario lavorativo dedicato ai giochi per computer sta assumendo proporzioni rilevanti. Pertanto è comprensibile che sempre più aziende prendano in considerazione la possibilità di eliminare i giochi dai computer utilizzati per lavoro.

Il programma AntiVir riconosce i giochi per computer. Se nella configurazione in Categorie delle minacce l'opzione **Giochi (GAMES)** è attivata con un segno di spunta, si riceve un avviso se il programma AntiVir ha eseguito un rilevamento. Il gioco è finito nel vero senso della parola visto che è possibile escluderlo facilmente.

Programmi ludici (JOKES)

I programmi ludici possono inorridire qualcuno o divertire tutti, senza essere dannosi o moltiplicarsi. La maggior parte delle volte il computer dopo il richiamo del programma ludico inizia a far suonare una melodia o a visualizzare qualcosa di insolito sullo schermo. Esempi di programmi ludici sono le lavatrici nel drive del floppy disk (DRAIN.COM) o il divoraschermo (BUGSRES.COM).

Ma attenzione! Tutte le manifestazioni di un programma ludico potrebbero anche essere prodotte da un virus o un trojan. L'effetto minimo sull'utente è uno spavento ma si può anche andare nel panico per la paura dei danni che possono verificarsi.

Il programma AntiVir è in grado di riconoscere i programmi ludici mediante un'estensione delle proprie routine di scansione ed eventualmente di eliminare il programma indesiderato. Se nella configurazione in Categorie delle minacce è stata attivata l'opzione **Programmi ludici (JOKES)** con un segno di spunta, si viene informati sui relativi rilevamenti.

Security Privacy Risk (SPR)

Software che minano la sicurezza del sistema, causano funzioni di programma non desiderate, violano la sfera privata o spiano il comportamento dell'utente e che sono quindi generalmente indesiderati.

Il programma AntiVir riconosce il software "Security Privacy Risk". Se nella configurazione in Categorie delle minacce l'opzione **Security Privacy Risk (SPR)** è attivata con un segno di spunta, si riceve un avviso se il programma AntiVir ha eseguito un rilevamento.

Software di controllo backdoor (BDC)

Per prelevare dati o manipolare il sistema viene inserito "dalla porta posteriore" un programma server backdoor senza che l'utente se ne accorga. Questo programma può essere gestito da terzi mediante Internet o la rete con un software di gestione backdoor (Client).

Il programma AntiVir riconosce il "Software di gestione Backdoor". Se nella configurazione in Categorie delle minacce l'opzione **Software di gestione Backdoor (BDC)** è attivata con un segno di spunta, si riceve un avviso se il programma AntiVir ha eseguito un rilevamento.

Adware/Spyware (ADSPY)

Software che visualizza messaggi pubblicitari o che invia i dati personali dell'utente, spesso a sua insaputa, a terzi e che risulta quindi indesiderato.

Il programma AntiVir riconosce l'"Adware/Spyware". Se nella configurazione in Categorie delle minacce è stata attivata l'opzione **Adware/Spyware (ADSPY)** con un segno di spunta, si riceve un avviso se il programma AntiVir ha eseguito un rilevamento.

Programmi zip runtime insoliti (PCK)

I file compressi con un programma zip runtime insolito possono essere identificati come sospetti.

Il programma AntiVir riconosce "Programmi zip runtime insoliti". Se nella configurazione in Categorie delle minacce l'opzione **Programmi zip runtime insoliti (PCK)** è attivata, si riceve un avviso quando il programma AntiVir effettua un rilevamento.

File con estensioni occultate (HEUR-DBLEXT)

File eseguibili che occultano la propria estensione in modo sospetto. Il metodo dell'occultamento viene spesso utilizzato dai malware.

Il programma AntiVir riconosce i "file con estensioni occultate". Se nella configurazione in Categorie delle minacce l'opzione **File con estensioni occultate (HEUR-DBLEXT)** è attivata con un segno di spunta, si riceve un avviso quando il programma AntiVir effettua un rilevamento.

Phishing

Il phishing, anche noto come *brand spoofing* è una forma raffinata di furto dei dati per i clienti o i potenziali clienti di provider Internet, banche, servizi di online banking, enti di registrazione.
Con la trasmissione dell'indirizzo email in Internet, la compilazione di moduli online, la partecipazione a newsgroup o siti web è possibile che vengano sottratti i dati dai cosiddetti "Internet crawling spiders" e utilizzati senza consenso per effettuare frodi o altre attività illegali.

Il programma AntiVir riconosce un tentativo di "phishing". Se nella configurazione in Categorie delle minacce l'opzione **Phishing** è attivata con un segno di spunta, si riceve un avviso quando il programma AntiVir rileva un tale comportamento.

Applicazione (APPL)

Con la denominazione APPL si intende un'applicazione il cui utilizzo può essere rischioso o la cui origine è dubbia.

Il programma AntiVir riconosce l'"applicazione (APPL)". Se nella configurazione in Categorie delle minacce l'opzione **Applicazione (APPL)** è attivata con un segno di spunta, si riceve un avviso quando il programma AntiVir rileva un tale comportamento.

11.2 Virus e altri malware

Adware

Con Adware si designa un software che mostra all'utente i banner e i pop up pubblicitari. Questi inserti pubblicitari generalmente non possono essere chiusi e sono quasi sempre visibili. I dati della connessione permettono numerosi feedback sul comportamento dell'utente e sono problematici per motivi di sicurezza dei dati.

Backdoor

Un Backdoor (italiano: porta posteriore) permette, aggirando la tutela all'accesso, di ottenere l'accesso a un computer.

Un programma in esecuzione di nascosto permette a un aggressore di godere di diritti pressoché illimitati. Con l'aiuto del backdoor i dati personali dell'utente possono essere spiati. I backdoor però vengono utilizzati soprattutto per installare altri virus o worm sul sistema infetto.

Virus dei record di avvio

Il record di avvio e il record master di avvio degli hard disk vengono inficiati di preferenza da virus dei record di avvio, che sovrascrivono informazioni importanti all'avvio del sistema. Una delle conseguenze spiacevoli: il sistema operativo non può più essere caricato...

Bot-Net

Per Bot-Net si intende una rete di PC gestibile a distanza (in Internet), composta da bot che comunicano l'uno con l'altro. Questo controllo si raggiunge con virus e trojan che inficiano il computer e poi aspettano indicazioni senza apportare danni al computer intaccato. Queste reti possono essere utilizzare per la diffusione di spam, attacchi DDoS, ecc., talvolta senza che gli utenti del PC si accorgano di alcunché. Il potenziale principale dei Bot-Net è quello di poter raggiungere reti di migliaia di computer, la cui portata salta gli accessi a Internet.

Exploit

Un Exploit (lacuna di sicurezza) è un programma del computer o uno script che sfrutta le debolezze specifiche o le funzioni errate di un sistema operativo o del programma. Una forma di Exploit sono gli attacchi da Internet con l'aiuto di pacchetti di dati manipolati, che sfruttano le debolezze nel software di rete. Con l'utilizzo di alcuni programmi che si introducono clandestinamente si ottiene un più ampio accesso.

Hoaxes (inglese: hoax - scherzo, burla)

Da un paio di anni gli utenti ricevono avvisi di virus che potrebbero diffondersi per email in Internet o in altre reti. Questi avvisi vengono distribuiti per email con la richiesta di inoltrarli a quanti più colleghi e utenti possibili per metterli in guardia sul "pericolo".

Honeypot

Un Honeypot (pentola di miele) è un servizio installato in una rete (programma o server). Esso ha il compito di monitorare una rete e registrare gli attacchi. Questo servizio è sconosciuto all'utente legittimo e quindi non viene mai toccato. Quando un aggressore cerca punti di debolezza in una rete e prende in considerazione i servizi offerti da un Honeypot viene registrato e viene emesso un allarme.

Macrovirus

I macrovirus sono piccoli programmi che sono scritti nella lingua delle macro di un'applicazione (ad esempio WordBasic in WinWord 6.0) e normalmente potrebbero diffondersi all'interno di documenti di questa applicazione. Essi vengono pertanto chiamati anche virus dei documenti. Per renderli attivi è necessario avviare l'applicazione corrispondente ed eseguire una delle macro infette. Diversamente dai virus "normali" i macrovirus non riguardano file eseguibili, ma documenti dell'applicazione host.

Pharming

Il pharming è una manipolazione del file host dei browser Web, per reindirizzare richieste dei siti Web falsificati. Si tratta di una rielaborazione del classico phishing. I truffatori che si servono del pharming godono di grandi quantità di server sui quali vengono archiviati i siti Web falsificati. Il pharming si è consolidato come iperonimo per diversi tipi di attacchi al DNS. In caso di manipolazione del file host con l'ausilio di un trojan o un virus viene effettuata una manipolazione del sistema. La conseguenza è che sono richiamabili solo siti Web falsificati da questo sistema, se l'indirizzo Web viene inserito correttamente.

Phishing

Phishing significa letteralmente pescare dati personali degli utenti di Internet. Il phisher invia generalmente alla vittima lettere aventi valore ufficiale, come ad esempio email che veicolano informazioni sensibili, soprattutto nomi utenti e password o PIN e TAN di accessi all'Online-Banking, approfittando della sua buona fede. Con i dati di accesso rubati il phisher assume l'identità della vittima e conduce operazioni a suo nome. Una cosa è certa: le banche e le assicurazioni non chiedono mai di inviare numeri di carte di credito, PIN, TAN o altri dati di accesso per email, SMS o telefonicamente.

Virus polimorfi

I veri campioni del mimetismo e del travestimento sono i virus polimorfi. Modificano i codici di programmazione e sono pertanto difficili da riconoscere.

Virus di programma

Un virus del computer è un programma che ha la capacità, una volta richiamato, di agganciarsi in qualche modo ad altri programmi e, da tale posizione, di inficiare il sistema. I virus si diffondono quindi in contrasto alle bombe logiche e ai trojan stessi. Al contrario di un worm, un virus ha bisogno di un programma estraneo ospite in cui archiviare il proprio codice virulento. Normalmente, la funzionalità del programma ospite non viene modificata.

Rootkit

Un Rootkit è un insieme di strumenti software che vengono installati su un computer dopo un'irruzione per nascondere il login dell'intruso, nascondere processi e registrare dati - in linea generale: per rendersi invisibile. I rootkit tentano di aggiornare i programmi spia già installati e di installare nuovamente gli spyware eliminati.

Virus di script e worm

Questi virus sono estremamente semplici da programmare e in poche ore si diffondono per email a livello globale, premesso che siano presenti tecniche ad hoc.

I virus di script e i worm utilizzano la lingua degli script, come ad esempio Javascript, VBScript ecc., per inserirsi in altri nuovi script o per diffondersi mediante il richiamo di funzioni del sistema operativo. Spesso ciò avviene tramite email o mediante lo scambio di file (documenti).

Il worm è un programma che non intacca alcun documento ospite. I worm non possono quindi divenire una componente di altri programmi. I worm rappresentano spesso l'unica possibilità di introdursi clandestinamente su sistemi dotati di provvedimenti restrittivi legati alla sicurezza.

Spyware

Gli spyware sono i cosiddetti programmi spia che inviano dati personali dell'utente a terzi senza che questi ne siano a conoscenza e senza l'approvazione del produttore del software. I programmi spyware servono soprattutto ad analizzare la navigazione in Internet e a introdurre banner o pop up pubblicitari in maniera mirata.

Cavalli di Troia (in breve trojan)

I trojan sono sempre più diffusi. Così vengono definiti i programmi che pretendono di avere una funzione precisa; dopo il loro avvio, tuttavia, mostrano il loro vero volto ed eseguono altre funzioni che hanno per lo più effetti distruttivi. I trojan non possono moltiplicarsi da soli e in questo si differenziano dai virus e dai worm. La maggior parte di loro ha un nome interessante (SEX.EXE o STARTME.EXE), che ha la funzione di spingere l'utente a eseguire il trojan. Subito dopo l'esecuzione diventano attivi e formattano, ad esempio, l'hard disk. Un tipo particolare di trojan è il dropper, che "lascia cadere" i virus, ovvero li installa nel sistema del computer.

Zombie

Un PC zombie è un calcolatore che è intaccato da programmi malware e permette all'hacker di abusare del computer mediante la gestione a distanza per fini criminali. Il PC infetto lancia il comando, ad esempio, di attacchi di Denial-of-Service- (DoS) o invia spam o email di phishing.

12 Info e Service

In questo capitolo si ottengono informazioni sui modi in cui è possibile tenersi in contatto con noi.

vedere capitolo Indirizzo di contatto

vedere capitolo Supporto tecnico

vedere capitolo File sospetto

vedere capitolo Comunicare un falso allarme

vedere capitolo Un suo feedback per una maggiore sicurezza

12.1 Indirizzi di contatto

Siamo a disposizione del cliente qualora avesse domande o suggerimenti sul mondo dei prodotti AntiVir. I nostri indirizzi dove contattarci sono disponibili in Control Center, sotto Guida in linea :: Informazioni su Avira Premium Security Suite.

12.2 Supporto tecnico

Il supporto Avira si rivolge all'utente in modo affidabile e serve a rispondere alle sue domande o a risolvere un problema tecnico.

Sul nostro sito Web l'utente può riferire tutte le informazioni utili per il nostro ampio servizio di supporto:

http://www.avira.it/supporto-premium-suite

Per poter ricevere aiuto nel modo migliore e più veloce possibile l'utente deve prendere in considerazione le seguenti informazioni:

– **Dati sulla licenza**. Esse si trovano sull'interfaccia del programma, alla voce del menu Guida in linea :: Informazioni su Avira Premium Security Suite :: Informazioni sulla licenza.
– **Informazioni sulla versione**. Esse si trovano sull'interfaccia del programma, alla voce del menu Guida in linea :: Informazioni su Avira Premium Security Suite :: Informazioni sulla licenza.
– **Versione del sistema operativo** e service pack eventualmente installati.
– **I pacchetti software installati**, ad esempio software antivirus di altri produttori.
– **Messaggi precisi** del programma o del file di report.

12.3 File sospetto

I virus che non possono essere riconosciuti o eliminati dai nostri prodotti così come i file sospetti possono essere inviati a noi. A tale scopo sono disponibili diverse modalità di invio.

– Selezionare il file nel Gestore della quarantena di Control Center e selezionare la voce Invia file mediante il menu contestuale o i pulsanti corrispondenti.
– Allegare il file desiderato compresso (WinZIP, PKZip, Arj, ecc.) ad un'email e inviarlo al seguente indirizzo:
  virus-premium-suite@avira.it
  Poiché alcuni Email-Gateways operano con software antivirus, si prega di proteggere il file/i file con una password (non dimenticare di comunicare anche la password).

In alternativa è possibile inviare il file sospetto mediante la nostra pagina web:
http://www.avira.it/file-upload

12.4 Comunicare un falso allarme

Se si ritiene che il proprio programma AntiVir abbia segnalato un rilevamento in un file che tuttavia con tutta probabilità è "pulito", si prega di inviare tale file compresso (WinZIP, PKZIP, Arj, ecc.) per email come allegato al seguente indirizzo:

– virus-premium-suite@avira.it

Poiché alcuni Email-Gateways operano con software antivirus, si prega di proteggere il file/i file con una password (non dimenticare di comunicare anche la password).

12.5 Un suo Feedback per una maggiore sicurezza

Per Avira la sicurezza degli utenti è al primo posto. Pertanto non disponiamo solamente di un team di esperti, a cui viene sottoposta ogni singola soluzione di Avira GmbH e ogni aggiornamento prima della pubblicazione dei test di sicurezza e qualità. Consigliamo di prendere seriamente le note su eventuali punti di debolezza rilevanti per la sicurezza e le si tratti chiaramente.

Se si ritiene che esista una lacuna rilevante per la sicurezza in uno dei nostri prodotti inviare un'email al seguente indirizzo:

vulnerabilities-premium-suite@avira.it

13 Riferimento: Opzioni di configurazione

Il riferimento della configurazione elenca le opzioni di configurazione disponibili.

13.1 Sistema di scansione

La rubrica Sistema di scansione della configurazione è dedicata alla configurazione della scansione diretta, ovvero alla scansione su richiesta.

13.1.1 Cerca

Qui si può definire la procedura standard della routine di scansione durante una scansione diretta. Se si seleziona una determinata directory da controllare durante la scansione diretta, il sistema di scansione esegue i controlli in base alla configurazione:

- con una determinata prestazione di scansione (priorità),
- anche sui record di avvio e nella memoria principale,
- su alcuni o tutti i record di avvio e nella memoria principale,
- su tutti i file o i file selezionati nella directory.

File

Il sistema di scansione può utilizzare un filtro per scansionare solamente i file con una determinata estensione (tipo).

Tutti i file

Se l'opzione è attivata, viene eseguita una ricerca di virus e programmi indesiderati in tutti i file, indipendentemente dal contenuto e dall'estensione. Il filtro non viene utilizzato.

Suggerimenti
Se Tutti i file è attivo, il pulsante **Estensioni dei file** non è selezionabile.

Utilizza estensioni smart

Se l'opzione è attivata, la selezione dei file da scansionare viene effettuata automaticamente dal programma. Ciò significa che il programma AntiVir decide in base al contenuto se un file deve essere controllato o meno per la presenza di virus e programmi indesiderati. Questa procedura è lievemente più lenta di Utilizza elenco estensione file, ma molto più sicura poiché i controlli non vengono effettuati solamente sulla base delle estensioni dei file. Questa opzione è attivata di default ed è consigliata.

Suggerimenti
Se Utilizza estensioni smart è attivo, il pulsante **Estensioni file** non può essere scelto.

Utilizza la lista delle estensioni

Se l'opzione è attivata, vengono scansionati solo i file con una determinata estensione. Sono preimpostati tutti i tipi di file che possono contenere virus e programmi indesiderati. L'elenco può essere modificato manualmente mediante il pulsante "**Estensioni file"**.

Suggerimenti
Se questa opzione è attivata e tutte le voci dell'elenco delle estensioni dei file sono state eliminate, viene visualizzato il testo "Nessuna estensione dei file" sotto il pulsante **Estensioni file**.

Estensioni file

Con questo pulsante viene richiamata una finestra di dialogo nella quale sono riportate tutte le estensioni dei file che vengono controllate durante una scansione in modalità "**Utilizza elenco estensioni file"**. Tra le estensioni sono presenti voci standard, ma è possibile anche aggiungere o eliminare voci.

Suggerimenti
Prestare attenzione al fatto che l'elenco standard può variare da versione a versione.

Impostazioni aggiuntive

Scansiona settori di avvio dei drive

Se l'opzione è attivata, il sistema di scansione controlla i record di avvio dei drive selezionati durante la scansione diretta. Questa opzione è attivata di default.

Scansione dei record master di avvio

Se l'opzione è attivata, il sistema di scansione controlla i record master di avvio degli/dell'hard disk utilizzati/o nel sistema.

Ignora i file offline

Se l'opzione è attivata, durante la scansione diretta i cosiddetti file offline vengono completamente ignorati. Ciò significa che in questi file non viene controllata la presenza di virus e programmi indesiderati. I file offline sono quei file che sono stati archiviati fisicamente dall'hard disk, per es. su un nastro, mediante il cosiddetto sistema gerarchico di gestione della memoria. Questa opzione è attivata di default.

Controllo di integrità dei file di sistema

Se l'opzione è attivata, i principali file di sistema Windows vengono sottoposti a una verifica particolarmente sicura durante ogni scansione diretta per verificare la presenza di modifiche dovute a malware. Se viene individuato un file modificato, questo viene segnalato come rilevamento sospetto. La funzionalità occupa molta memoria. Per questo motivo l'opzione è disattivata di default.

Importante
L'opzione è disponibile solo a partire da Windows Vista.

Suggerimenti
Se si utilizzano strumenti di terzi, si modificano i file di sistema o si personalizza la schermata di avvio, questa opzione non deve essere utilizzata. Questi strumenti sono, ad esempio, i cosiddetti skinpack, TuneUp Utilities o Vista Customization.

Scansione ottimizzata

Se l'opzione è attivata, la capacità del processore viene utilizzata in modo ottimale durante la scansione con il sistema di scansione. Per motivi di performance, in caso di scansione ottimale, la funzione di report si verifica al massimo a un livello standard.

Suggerimenti
L'opzione è disponibile solo per computer multiprocessore.

Seguire link simbolici

Se l'opzione è attivata, il sistema di scansione esegue una scansione di tutti i collegamenti simbolici nel profilo di ricerca o nelle directory selezionate, allo scopo di scansionare i file collegati alla ricerca di virus e malware. Questa opzione non è supportata in Windows 2000 ed è disattivata di default.

Importante
L'opzione non comprende i collegamenti (shortcut), bensì si riferisce esclusivamente ai link simbolici (generati con mklink.exe) o ai punti di giunzione (generati con junction.exe), presenti in modalità trasparente nel file system.

Scansione rootkit all'avvio

Se l'opzione è attivata, il sistema di scansione verifica con una scansione all'avvio la directory di sistema Windows tramite una procedura rapida per verificare la presenza di eventuali rootkit attivi. Questa procedura non verifica se nel computer vi sono rootkit attivi così dettagliatamente come il profilo di ricerca "**Cerca rootkit**", ma è molto più rapida.

Importante
Scansione rootkit in Windows XP 64 Bit non disponibile!

Scansiona registro

Se l'opzione è attivata, viene scansionato il registro alla ricerca di software dannosi.

Processo di scansione

Permetti di arrestare sist. di scansione

Se l'opzione è attivata, la ricerca di virus o programmi indesiderati può essere arrestata in ogni momento con il pulsante "**Arresta"** nella finestra "Luke Filewalker". Se questa impostazione è disattivata, il pulsante **Arresta** nella finestra "Luke Filewalker" è grigio. Pertanto non è possibile terminare prematuramente una scansione! Questa opzione è attivata di default.

Priorità del sistema di scansione

Il sistema di scansione differenzia tre livelli di priorità nella scansione diretta. Si tratta di un sistema efficace solo se sul computer sono in esecuzione più processi contemporaneamente. La scelta si ripercuote anche sulla velocità di scansione.

Livello basso

Il sistema di scansione riceve dal sistema operativo il tempo del processore solo se nessun altro processo necessita di tempo di elaborazione, ovvero finché il sistema di scansione è l'unico programma in esecuzione, la velocità è massima. Nel complesso, in questo modo viene gestito molto bene anche il lavoro con altri programmi: il computer è più veloce se altri programmi sono in esecuzione, mentre il sistema di scansione lavora in background. Questa opzione è attivata di default ed è consigliata.

Livello medio

Il sistema di scansione viene eseguito con priorità normale. Tutti i processi ricevono lo stesso tempo di elaborazione dal sistema operativo. In alcune circostanze il lavoro con altre applicazioni ne risulta compromesso.

Livello elevato

Il sistema di scansione riceve la massima priorità. Un lavoro parallelo con altre applicazioni è pressoché impossibile. Tuttavia il sistema completa la scansione in maniera estremamente rapida.

13.1.1.1. Azione per i rilevamenti

Azione per i rilevamenti

È possibile definire azioni che il sistema di scansione deve eseguire quando viene rilevato un virus o un programma indesiderato.

Interattivo

Se l'opzione è attivata, i rilevamenti della scansione del sistema vengono notificati in una finestra di dialogo. Al termine della scansione, si riceve un avviso con l'elenco dei file infetti rilevati. Mediante il menu contestuale è possibile selezionare un'azione da eseguire per i singoli file infetti. È possibile eseguire l'azione selezionata per tutti i file infetti oppure interrompere la scansione.

Suggerimenti
Di default nella finestra di dialogo è preselezionata l'azione 'Sposta in quarantena'. È possibile selezionare ulteriori azioni mediante il menu contestuale.

É possibile reperire maggiori informazioni qui.

Automatico

Se l'opzione è attivata, in caso di rilevamento di un virus o di programmi indesiderati non appare alcuna finestra di dialogo in cui selezionare l'azione da eseguire. Il sistema di scansione reagisce conformemente alle impostazioni effettuate precedentemente dall'utente in questa sezione.

Backup in quarantena

Se l'opzione è attivata, il sistema di scansione crea una copia di sicurezza (backup) prima dell'esecuzione delle azioni primarie e secondarie desiderate. La copia di sicurezza viene mantenuta in Quarantena dove il file può essere ripristinato se possiede un valore dimostrativo. Inoltre è possibile inviare la copia di sicurezza ad Avira Malware Research Center per ulteriori indagini.

Azione primaria

L'azione primaria è l'azione che viene eseguita quando il sistema di scansione rileva un virus o un programma indesiderato. Se l'opzione "**ripara"** è attiva, ma la riparazione del file infetto non è possibile, verrà eseguita l'azione definita in"**Azione secondaria"**.

Suggerimenti
L'opzione **azione secondaria** è selezionabile solo se in **azione primaria** è stata selezionata l'impostazione**ripara**.

ripara

Se l'opzione è attivata, il sistema di scansione ripara automaticamente i file infetti. Se il sistema di scansione non può riparare un file infetto, in alternativa esegue l'opzione selezionata in Azione secondaria.

Suggerimenti
Si consiglia una riparazione automatica, che tuttavia comporta una modifica dei file presenti sul computer da parte del sistema di scansione.

elimina

Se l'opzione è attivata, il file viene eliminato. Questa procedura è più rapida di "sovrascrivi ed elimina".

sovrascrivi ed elimina

Se l'opzione è attivata, il sistema di scansione sovrascrive il file con un modello standard, infine lo elimina. Il file non può essere ripristinato.

rinomina

Se l'opzione è attivata, il sistema di scansione rinomina il file. Non sarà quindi più possibile accedere direttamente ai file (ad esempio con un doppio clic). I file possono essere riparati successivamente e nuovamente rinominati.

ignora

Se l'opzione è attivata, l'accesso al file viene consentito e il file viene mantenuto.

Attenzione
Il file infetto rimane attivo sul computer! Questo potrebbe causare danni notevoli al computer!

quarantena

Se l'opzione è attivata, il sistema di scansione sposta il file in quarantena. I file possono essere riparati successivamente o, se necessario, inviati ad Avira Malware Research Center.

Azione secondaria

L'opzione "**Azione secondaria"** è selezionabile solo se in "**Azione primaria"** è stata selezionata l'impostazione **Ripara**. Con questa opzione si può decidere cosa fare con il file infetto se non è riparabile.

elimina

Se l'opzione è attivata, il file viene eliminato. Questa procedura è più rapida di "sovrascrivi ed elimina".

sovrascrivi ed elimina

Se l'opzione è attivata, il sistema di scansione sovrascrive il file con un modello standard, infine lo elimina (wipe). Il file non può essere ripristinato.

rinomina

Se l'opzione è attivata, il sistema di scansione rinomina il file. Non sarà quindi più possibile accedere direttamente ai file (ad esempio con un doppio clic). I file possono essere riparati successivamente e nuovamente rinominati.

ignora

Se l'opzione è attivata, l'accesso al file viene consentito e il file viene mantenuto.

Attenzione
Il file infetto rimane attivo sul computer! Questo potrebbe causare danni notevoli al computer!

quarantena

Se l'opzione è attivata, il sistema di scansione sposta il file in quarantena. I file possono essere riparati successivamente o, se necessario, inviati ad Avira Malware Research Center.

Suggerimenti
Se si seleziona **Elimina** o **Sovrascrivi ed elimina** come azione principale o secondaria, attenersi alle seguenti indicazioni: in caso di rilevamento di oggetti euristici, i file infetti non vengono eliminati, bensì spostati in quarantena.

Per la ricerca negli archivi il sistema di scansione utilizza una scansione ricorsiva: vengono decompressi anche gli archivi in altri archivi e viene controllata la presenza di virus e programmi indesiderati. I file compressi vengono scansionati, decompressi e nuovamente scansionati.

Scansiona archivi

Se l'opzione è attivata, vengono scansionati gli archivi selezionati nell'elenco degli archivi. Questa opzione è attivata di default.

Tutti i tipi di archivio

Se l'opzione è attivata, vengono selezionati e scansionati i tipi di archivi nella lista di archivi.

Smart Extension

Se l'opzione è attivata, il sistema di scansione riconosce se un file è in formato compresso (archivio), anche se l'estensione è diversa da quelle abituali, e scansiona l'archivio. Tuttavia a tal fine ogni file deve essere aperto, riducendo così la velocità della scansione. Esempio: se un archivio *.zip ha estensione *.xyz, il sistema di scansione decomprime anche tale archivio e lo scansiona. Questa opzione è attivata di default.

Suggerimenti
Vengono scansionati solo quei tipi di archivio che sono selezionati nell'elenco degli archivi.

Limita la profondità di ricorsione

La decompressione e la scansione di archivi particolarmente ramificati può necessitare di molto tempo e molte risorse del sistema. Se l'opzione è attivata, è possibile limitare la profondità della scansione in archivi multipli a un determinato numero di livelli di compressione (profondità di ricorsione massima). In questo modo è possibile risparmiare tempo e risorse del processore.

Suggerimenti
Per individuare un virus o un programma indesiderato all'interno di un archivio, il sistema di scansione deve eseguire la scansione fino al livello di ricorsione nel quale si trova il virus o il programma indesiderato.

Profondità massima di ricorsione

Per poter indicare la profondità massima di ricorsione l'opzione Limita profondità di ricorsione deve essere attivato.
È possibile inserire direttamente la profondità di ricorsione desiderata oppure modificarla per mezzo dei tasti freccia a destra del campo. I valori consentiti sono compresi tra 1 e 99. Il valore standard e consigliato è 20.

Valori predefiniti

Il pulsante crea i valori predefiniti per la scansione degli archivi.

Elenco archivi

In questa sezione è possibile impostare quali archivi devono essere scansionati dal sistema di scansione. A tal fine è necessario attivare le voci corrispondenti.

13.1.1.2. Eccezioni

Oggetti file da escludere dalla scansione

L'elenco in questa finestra contiene file e percorsi che non devono essere presi in considerazione dal sistema di scansione durante la ricerca di virus e programmi indesiderati.

Si consiglia di inserire quante meno eccezioni possibili e solo i file che non devono essere scansionati durante una scansione normale per qualsivoglia motivo. Consigliamo di far comunque controllare la presenza di virus o programmi indesiderati in questi file prima di inserirli in questo elenco!

Suggerimenti
Le voci dell'elenco non possono superare complessivamente i 6000 caratteri.

Attenzione
Questi file non vengono presi in considerazione durante la scansione!

Suggerimenti
I file inseriti in questa lista vengono segnalati nel file di report. Controllare di tanto in tanto nel file di report la presenza di questi file non scansionati poiché potrebbe non sussistere più il motivo per il quale sono stati esclusi. In questo caso i nomi di questi file dovrebbero essere eliminati dall'elenco.

Campo

Inserire in questo campo il nome del file che non deve essere preso in considerazione durante una scansione diretta. Di default non è indicato alcun file.

Il pulsante apre una finestra nella quale si ha la possibilità di selezionare il file o il percorso desiderato.
Se si è fornito un nome di file con un percorso completo, tale file non viene scansionato. Se si è inserito un nome di file senza un percorso, ogni file con tale nome (indipendentemente dal percorso o dal drive) non verrà scansionato.

Aggiungi

Con il pulsante è possibile accettare il file indicato nel campo nella finestra di visualizzazione.

Elimina

Il pulsante elimina una voce selezionata nella lista. Questo pulsante non è attivo se non è selezionata alcuna voce.

Suggerimenti
Se si aggiunge un'intera partizione all'elenco dei file da escludere, verranno tralasciati dalla scansione solo i file salvati direttamente nella partizione e non i file contenuti in directory all'interno della partizione:
Esempio: file da omettere: `D:\ = D:\file.txt` verrà tralasciato dalla scansione del sistema, invece `D:\folder\file.txt` verrà incluso nella scansione.

13.1.1.3. Euristico

Questa rubrica di configurazione contiene le impostazioni per l'euristica del motore di ricerca.

I prodotti AntiVir contengono un'euristica molto efficace, che consente di riconoscere in modo proattivo malware sconosciuti, ovvero prima che venga creata una firma speciale dei virus contro il parassita e che venga inviato un aggiornamento della protezione antivirus. Il riconoscimento dei virus avviene attraverso un'approfondita analisi e indagine del relativo codice in base alle funzioni tipiche dei malware. Se il codice esaminato corrisponde a tali caratteristiche tipiche viene segnalato come sospetto. Ciò non significa necessariamente che il codice indichi effettivamente la presenza di un malware; potrebbe trattarsi anche di messaggi di errore. La decisione su come procedere con il codice spetta all'utente stesso, ad esempio sulla base delle sue conoscenze relativamente all'attendibilità della fonte che contiene il codice segnalato.

Macrovirus euristico

Macrovirus euristico

Il prodotto AntiVir acquistato contiene un macrovirus euristico molto efficace. Se l'opzione è attivata, in caso di riparazione possibile tutte le macro del documento infetto vengono eliminate, in alternativa i documenti sospetti vengono solo segnalati, l'utente riceverà quindi un avviso. Questa impostazione è attivata di default e viene consigliata.

Advanced Heuristic Analysis and Detection (AHeAD)

Attiva AHeAD

Il programma AntiVir contiene, grazie alla tecnologia AntiVir AHeAD, un'euristica molto efficace, in grado di riconoscere anche malware sconosciuti (nuovi). Se l'opzione è attivata, è possibile impostare il grado di rigidità dell'euristica. Questa opzione è attivata di default.

Livello di rilevamento basso

Se l'opzione è attivata, viene riconosciuto un numero inferiore di malware sconosciuti e il rischio di possibili rilevamenti di errore è limitato.

Livello di rilevamento medio

Questa impostazione è attivata di default, se è stata scelta l'applicazione di questa euristica.

Livello di riconoscimento elevato

Se l'opzione è attivata, viene riconosciuto un numero significativamente maggiore di malware sconosciuti, ma possono verificarsi messaggi di errore.

13.1.2 Report

Il sistema di scansione possiede una funzione di log molto ampia. In questo modo si ricevono informazioni esatte sui risultati di una scansione diretta. Il file di report contiene tutte le voci del sistema e gli avvisi e i messaggi della scansione diretta.

Suggerimenti
Per comprendere quali azioni il sistema di scansione ha eseguito in caso di rilevamento di virus o programmi indesiderati, deve sempre essere creato un file di report.

Funzione di log

Disabilitato

Se l'opzione è attivata, il sistema di scansione non riporta le azioni e i risultati della scansione diretta.

Standard

Se l'opzione è attivata, il sistema di scansione riporta il nome dei file infetti con il percorso. Inoltre, la configurazione per la scansione attuale, le informazioni sulla versione e sul proprietario della licenza viene riportata nel file di report.

Avanzato

Se l'opzione è attivata, il sistema di scansione riporta anche gli avvisi e le note, oltre alle informazioni standard.

Completo

Se l'opzione è attivata, il sistema di scansione riporta tutti i file scansionati. Inoltre, tutti i file infetti, nonché gli avvisi e le note vengono registrati nel file di report.

Suggerimenti
Se l'utente deve inviare un file di report ad Avira (per la ricerca dell'errore), preghiamo di creare il file di report con questa modalità.

13.2 Guard

La rubrica Guard della configurazione è dedicata alla configurazione della scansione in tempo reale.

13.2.1 Cerca

Solitamente si desidera che il proprio sistema sia costantemente monitorato. Per questo viene utilizzato il Guard (scansione in tempo reale = On-Access Scanner). In questo modo è possibile ricercare la presenza di virus e programmi indesiderati in tutti i file che vengono aperti o copiati sul computer, "on the fly".

Modalità di scansione

Qui si stabilisce il momento in cui effettuare la scansione di un file.

Scansione in lettura

Se l'opzione è attivata, il Guard scansiona i file prima che vengano letti o eseguiti da un'applicazione o dal sistema operativo.

Scansione in scrittura

Se l'opzione è attivata, il Guard scansiona un file in scrittura. Dopo questa procedura è possibile accedere nuovamente al file.

Scansione in lettura e scrittura

Se l'opzione è attivata, il Guard scansiona i file prima dell'apertura, della lettura e dell'esecuzione e dopo la scrittura. Questa impostazione è attivata di default e viene consigliata.

File

Il Guard può utilizzare un filtro per scansionare solo i file con una determinata estensione (tipo).

Tutti i file

Se l'opzione è attivata, viene eseguita una ricerca di virus e programmi indesiderati in tutti i file, indipendentemente dal contenuto e dall'estensione.

Suggerimenti
Se Tutti i file è attivo, il pulsante **Estensioni dei file** non è selezionabile.

Utilizza estensioni smart

Se l'opzione è attivata, la selezione dei file da scansionare viene effettuata automaticamente dal programma. Ciò significa che il programma decide in base al contenuto se un file deve essere controllato o meno per la presenza di virus e programmi indesiderati. Questa procedura è lievemente più lenta di Utilizza lista estensione file, ma molto più sicura poiché i controlli non sono effettuati solamente sulla base delle estensioni dei file.

Suggerimenti
Se Utilizza estensioni smart è attivo, il pulsante **Estensioni file** non può essere scelto.

Utilizza la lista delle estensioni

Se l'opzione è attivata, vengono scansionati solo i file con una determinata estensione. Sono preimpostati tutti i tipi di file che possono contenere virus e programmi indesiderati. La lista può essere modificata manualmente mediante il pulsante "**Estensioni file"**. Questa opzione è attivata di default ed è consigliata.

Suggerimenti
Se questa opzione è attivata e tutte le voci dell'elenco delle estensioni dei file sono state eliminate, viene visualizzato il testo "Nessuna estensione dei file" sotto il pulsante **Estensioni file**.

Estensioni file

Con questo pulsante viene richiamata una finestra di dialogo nella quale vengono visualizzate le estensioni dei file che vengono controllate durante una scansione in modalità "**Utilizza lista estensione file"**. Tra le estensioni sono presenti voci standard, ma è possibile anche aggiungere o eliminare voci.

Suggerimenti
Prestare attenzione al fatto che l'elenco estensioni dei file può variare da versione a versione.

Archivi

Scansiona archivi

Se l'opzione è attivata, vengono scansionati gli archivi. I file compressi vengono scansionati, decompressi e nuovamente scansionati. Questa opzione è disattivata di default. La scansione degli archivi viene limitata dalla profondità di ricorsione, dal numero di file da scansionare e dalle dimensioni dell'archivio. È possibile impostare la profondità di ricorsione, il numero di file da scansionare e le dimensioni massime dell'archivio.

Suggerimenti
L'opzione è disattivata di default poiché il processo occupa molta memoria. Generalmente si consiglia di scansionare gli archivi con la scansione diretta.

Profondità massima di ricorsione

Per la ricerca negli archivi il Guard utilizza una scansione ricorsiva: vengono decompressi anche gli archivi in altri archivi e viene controllata la presenza di virus e programmi indesiderati. L'utente può stabilire la profondità di ricorsione. Il valore standard per la profondità di ricorsione è 1 ed è quello consigliato: tutti gli archivi che si trovano direttamente nell'archivio principale vengono scansionati.

Numero massimo dei file

Per la ricerca negli archivi la scansione viene limitata a un numero massimo di file dell'archivio. Il valore standard per il numero massimo di file da scansionare è 10 e viene consigliato.

Dimensione massima (KB)

Per la ricerca negli archivi la scansione viene limitata a una dimensione degli archivi massima, da decomprimere. Il valore standard è 1000 KB ed è consigliato.

13.2.1.1. Azione per i rilevamenti

Azione per i rilevamenti

È possibile stabilire delle azioni che il Guard deve eseguire quando viene rilevato un virus o un programma indesiderato.

Interattivo

Se l'opzione è attivata, in caso di rilevamento di un virus da parte del Guard compare un messaggio sul desktop. È possibile rimuovere il malware rilevato, oppure richiamare altre azioni possibili per il trattamento del virus selezionando il pulsante 'Dettagli'. Le azioni vengono visualizzate in una finestra di dialogo. Questa opzione è attivata di default.

É possibile reperire maggiori informazioni qui.

Automatico

Se l'opzione è attivata, in caso di rilevamento di un virus o di programmi indesiderati non appare alcuna finestra di dialogo in cui selezionare l'azione da eseguire. Il Guard reagisce conformemente alle impostazioni effettuate precedentemente dall'utente in questa sezione.

Backup in quarantena

Se l'opzione è attivata, il Guard crea una copia di sicurezza (backup) prima dell'esecuzione delle azioni primarie e secondarie desiderate. La copia di sicurezza viene conservata in quarantena. Il file può essere ripristinato dal Gestore della quarantena se ha un valore informativo. Inoltre è possibile inviare la copia di sicurezza ad Avira Malware Research Center. In base all'oggetto sono disponibili altre possibilità di scelta nelGestore della quarantena.

Azione primaria

L'azione primaria è l'azione che viene eseguita quando Guard rileva un virus o un programma indesiderato. Se l'opzione "**ripara**" è attiva, ma la riparazione del file infetto non è possibile, verrà eseguita l'azione definita in"**Azione secondaria**".

Suggerimenti
L'opzione azione secondaria è selezionabile solo se in azione primaria è stata selezionata l'impostazioneripara.

ripara

Se l'opzione è attivata, il Guard ripara automaticamente i file infetti. Se il Guard non può riparare un file infetto, in alternativa esegue l'opzione selezionata in Azione secondaria.

Suggerimenti
Si consiglia una riparazione automatica, questo comporta tuttavia una modifica dei file presenti sul computer da parte del Guard.

elimina

Se l'opzione è attivata, il file viene eliminato. Questa procedura è più rapida di "sovrascrivi ed elimina".

sovrascrivi ed elimina

Se l'opzione è attivata, il Guard sovrascrive il file con un modello predefinito, infine lo elimina. Il file non può essere ripristinato.

rinomina

Se l'opzione è attivata, il Guard rinomina il file. Non sarà quindi più possibile accedere direttamente ai file (ad esempio con un doppio clic). I file possono essere riparati successivamente e nuovamente rinominati.

ignora

Se l'opzione è attivata, l'accesso al file viene consentito e il file viene mantenuto.

Attenzione
Il file infetto rimane attivo sul computer! Questo potrebbe causare danni notevoli al computer!

Nega accesso

Se l'opzione è attivata, il Guard inserisce il rilevamento solo nel file di report, se la funzione di report è attivata. Inoltre, il Guard inserisce una voce nel Log eventi, se questa opzione è attivata.

quarantena

Se l'opzione è attivata, il Guard sposta il file nella directory di quarantena. I file in questa directory possono essere riparati successivamente o, se necessario, inviati ad Avira Malware Research Center.

Azione secondaria

L'opzione "**Azione secondaria"** è disponibile solo se in "**Azione primaria"** è stata selezionata l'opzione **"Ripara"**. Con questa opzione si può decidere come procedere con il file infetto se non è riparabile.

elimina

Se l'opzione è attivata, il file viene eliminato. Questa procedura è più rapida di "sovrascrivi ed elimina".

sovrascrivi ed elimina

Se l'opzione è attivata, il Guard sovrascrive il file con un modello predefinito, infine lo elimina. Il file non può essere ripristinato.

rinomina

Se l'opzione è attivata, il Guard rinomina il file. Non sarà quindi più possibile accedere direttamente ai file (ad esempio con un doppio clic). I file possono essere riparati successivamente e nuovamente rinominati.

ignora

Se l'opzione è attivata, l'accesso al file viene consentito e il file viene mantenuto.

Attenzione
Il file infetto rimane attivo sul computer! Questo potrebbe causare danni notevoli al computer!

Nega accesso

Se l'opzione è attivata, il Guard inserisce il rilevamento solo nel file di report, se la funzione di report è attivata. Inoltre, il Guard inserisce una voce nel Log eventi, se questa opzione è attivata.

quarantena

Se l'opzione è attivata, il Guard sposta il file in Quarantena. I file possono essere riparati successivamente o, se necessario, inviati ad Avira Malware Research Center.

Suggerimenti
Se si seleziona **Elimina** o **Sovrascrivi ed elimina** come azione primaria o secondaria, attenersi alle seguenti indicazioni: in caso di rilevamento di oggetti euristici, i file infetti non vengono eliminati, bensì spostati in quarantena.

13.2.1.2. Altre azioni

Notifiche

Log eventi

Utilizza il log degli eventi

Se l'opzione è attivata, viene inserita una voce nel log eventi di Windows a ogni rilevamento. È possibile richiamare gli eventi nel visualizzatore eventi di Windows. Questa opzione è attivata di default.

Avvio automatico

Blocca avvio automatico

Se l'opzione è attivata, l'avvio automatico di Windows viene bloccato su tutti i drive collegati, come penne USB, CD e DVD, drive di rete. Con la funzione di avvio automatico di Windows, i file sui supporti informatici o sui drive di rete vengono letti immediatamente al momento dell'inserimento o del collegamento; in questo modo i file possono essere avviati e riprodotti automaticamente. Tuttavia questa funzionalità nasconde un rischio per la sicurezza molto elevato, poiché con l'avvio automatico dei file è possibile che vengano installati malware e programmi indesiderati. Particolarmente critica è la funzione di avvio automatico delle penne USB poiché su questi supporti i file possono modificarsi continuamente.

Escludi CD e DVD

Se l'opzione è attivata, è consentita la funzione di avvio automatico sui drive CD e DVD.

Attenzione
Disattivare la funzione di avvio automatico per i drive CD e DVD solo se si è sicuri che si tratti di supporti informatici assolutamente affidabili.

13.2.1.3. Eccezioni

Con queste opzioni è possibile configurare gli oggetti soggetti a eccezioni per il Guard (scansione in tempo reale). Gli oggetti identificati verranno così esclusi dalla scansione in tempo reale. Il Guard può ignorare gli accessi ai file riportati nell'elenco dei processi da tralasciare durante la scansione in tempo reale. Questa funzione è utile ad esempio per le banche dati o le soluzioni di backup.
Nell'indicare i processi e gli oggetti file da escludere, prestare attenzione a quanto segue: L'elenco viene elaborato dall'alto verso il basso. Più lungo è l'elenco, maggiore è il tempo di cui il processore ha bisogno per elaborare l'elenco a ogni accesso. Si consiglia pertanto di mantenere l'elenco più breve possibile.

Processi da omettere per il Guard

Tutti gli accessi ai file dei processi indicati in questo elenco sono stati esclusi dal monitoraggio mediante il Guard.

Campo

Inserire in questo campo il nome del processo che deve essere ignorato dalla scansione in tempo reale. Di default non è indicato alcun processo.

Suggerimenti
È possibile inserire fino a 128 processi.

Suggerimenti
Pr indicare i processi è possibile utilizzare caratteri Unicode. Pertanto, è possibile indicare nomi di processi o directory che contengono caratteri speciali.

Suggerimenti
È possibile escludere dal monitoraggio di Guard i processi senza percorso completo: applicazione.exe
Ciò è valido solo per i processi i cui file eseguibili si trovano sul drive dell'hard disk.
Non indicare alcuna eccezione per i processi i cui file eseguibili si trovano su drive dinamici. I drive dinamici vengono utilizzati per i supporti dati rimovibili, quali CD, DVD o penna USB.

Suggerimenti
I drive devono essere indicati nel modo seguente: [Lettera del drive]:\
Il simbolo dei due punti (:) deve essere utilizzato solo per indicare il drive.

Suggerimenti
Per indicare il processo, è possibile utilizzare la wildcard * (numero a piacere di caratteri) e ? (un unico carattere):
C:\Programmi\Applicazioni\applicazione.exe
C:\Programmi\Applicazioni\applicazion?.exe
C:\Programmi\Applicazioni\applicaz*.exe
C:\Programmi\Applicazioni*.exe
Per evitare che l'intero processo venga escluso dal monitoraggio di Guard, i dati che contengono esclusivamente i seguenti caratteri non sono validi: * (asterisco), ? (punto interrogativo), / (barra), \ (barra rovesciata), . (punto), : (due punti).

Suggerimenti
Il percorso indicato e il nome del file del processo non possono superare i 255 caratteri. Le voci dell'elenco non possono superare complessivamente i 6000 caratteri.

Attenzione
Prestare attenzione al fatto che tutti gli accessi ai file dei processi che sono stati evidenziati nell'elenco sono esclusi dalla scansione di virus e programmi indesiderati! Esplora risorse di Windows e il sistema operativo non possono essere esclusi. La voce corrispondente nell'elenco viene ignorata.

Il pulsante apre una finestra nella quale si ha la possibilità di selezionare un file eseguibile.

Processi

Il pulsante "**Processi**" apre la finestra "*Selezione del processo*", in cui vengono indicati i processi in corso.

Aggiungi

Con il pulsante è possibile è possibile accettare il processo indicato nella finestra di visualizzazione.

Elimina

Con il pulsante si elimina un processo selezionato dalla finestra di visualizzazione.

Oggetti file da omettere per il Guard

Tutti gli accessi ai file degli oggetti indicati in questo elenco sono esclusi dal monitoraggio mediante il Guard.

Campo

Inserire in questo campo il nome del file che deve essere ignorato dalla scansione in tempo reale. Di default non è indicato alcun file.

Suggerimenti
Per indicare i file da omettere, è possibile utilizzare la wildcard * (numero a piacere di caratteri) e ? (un unico carattere). È possibile anche escludere singole estensioni di file (incluse le wildcard):
C:\directory*.mdb
*.mdb
*.md?
.xls
C:\directory*.log

Suggerimenti
I nomi delle directory devono concludersi con una barra inversa \, altrimenti viene confuso con un nome di file.

Suggerimenti
Le voci dell'elenco non possono superare complessivamente i 6000 caratteri.

Suggerimenti
Se una directory viene esclusa, anche tutte le sottodirectory che contiene vengono escluse automaticamente.

Suggerimenti
Per ogni drive è possibile indicare al massimo 20 eccezioni con il percorso completo (che inizia con la lettera del drive).
Es.: C:\Programmi\Applicazioni\Nome.log

Il numero massimo di eccezioni senza percorso completo è 64.
Ad es.: *.log

Suggerimenti
In caso di drive dinamici, collegati (montati) come directory a un altro drive, è necessario utilizzare nell'elenco delle eccezioni il nome dell'alias del sistema operativo per il drive collegato:
ad es. \Device\HarddiskDmVolumes\PhysicalDmVolumes\BlockVolume1\
Anche utilizzando il punto di montaggio stesso (mount point), ad es. C:\DynDrive, si esegue comunque la scansione del drive dinamico. È possibile ricavare i nomi dell'alias del sistema operativo da utilizzare dal file di report del Guard.

Il pulsante apre una finestra nella quale si ha la possibilità di selezionare i file da tralasciare.

Aggiungi

Con il pulsante è possibile accettare il file indicato nel campo nella finestra di visualizzazione.

Elimina

Con il pulsante si elimina un file selezionato dalla finestra di visualizzazione.

Per indicare le eccezioni, attenersi alle seguenti indicazioni:

Suggerimenti
Per escludere oggetti anche quando vi si accede con nomi di file DOS brevi (convenzione dei nomi di DOS 8.3), è necessario inserire nell'elenco il nome breve del file corrispondente.

Suggerimenti
Un nome di file che contiene wildcard non deve concludersi con una barra inversa.

Ad esempio:

```
C:\Programmi\Applicazione\applic*.exe\
```

Questa voce non è valida e non viene considerata come un'eccezione!

Suggerimenti
In base al file di report del Guard è possibile ricavare i percorsi utilizzati dal Guard durante la ricerca dei file infetti. Nell'elenco delle eccezioni, utilizzare di massima gli stessi percorsi. Procedere come segue: impostare la funzione di protocollo del Guard nella configurazione in Guard :: Report su **Completa**. Quindi accedere con il Guard attivato a file, directory, drive collegati . È ora possibile leggere il percorso da utilizzare dal file di report del Guard. È possibile richiamare il file di report nel Control Center in Protezione locale :: Guard.

Esempio dei processi da escludere:

– applicazione.exe

  Il processo di applicazione.exe viene escluso dalla scansione di Guard indipendentemente dal drive dell'hard disk o della directory applicazione.exe in cui si trova.

– C:\Programmi1\applicazione.exe

  Il processo del file applicazione.exe, che si trova nel percorso C:\Programmi1, viene escluso dalla scansione di Guard.

– C:\Programmi1*.exe

Tutti i processi dei file eseguibili, che si trovano nel percorso C:\Programmi1, vengono esclusi dalla scansione di Guard.

Esempio dei file da escludere:

– *.mdb

Tutti i file con estensione "mdb" vengono esclusi dalla scansione di Guard.

– *.xls*

Tutti i file la cui estensione inizia per "xls" vengono esclusi dalla scansione di Guard, ad esempio i file con estensione .xls e xlsx.

– C:\directory*.log

Tutti i file di registro con estensione "log", che si trovano nel percorso C:\directory, vengono esclusi dalla scansione di Guard.

-

13.2.1.4. Euristico

Questa rubrica di configurazione contiene le impostazioni per l'euristica del motore di ricerca.

I prodotti AntiVir contengono un'euristica molto efficace, che consente di riconoscere in modo proattivo malware sconosciuti, ovvero prima che venga creata una firma speciale dei virus contro il parassita e che venga inviato un aggiornamento della protezione antivirus. Il riconoscimento dei virus avviene attraverso un'approfondita analisi e indagine del relativo codice in base alle funzioni tipiche dei malware. Se il codice esaminato corrisponde a tali caratteristiche tipiche viene segnalato come sospetto. Ciò non significa necessariamente che il codice indichi effettivamente la presenza di un malware; potrebbe trattarsi anche di messaggi di errore. La decisione su come procedere con il codice spetta all'utente stesso, ad esempio sulla base delle sue conoscenze relativamente all'attendibilità della fonte che contiene il codice segnalato.

Macrovirus euristico

Macrovirus euristico

Il prodotto AntiVir acquistato contiene un macrovirus euristico molto efficace. Se l'opzione è attivata, in caso di riparazione possibile tutte le macro del documento infetto vengono eliminate, in alternativa i documenti sospetti vengono solo segnalati, l'utente riceverà quindi un avviso. Questa impostazione è attivata di default e viene consigliata.

Advanced Heuristic Analysis and Detection (AHeAD)

Attiva AHeAD

Il programma AntiVir contiene, grazie alla tecnologia AntiVir AHeAD, un'euristica molto efficace, in grado di riconoscere anche malware sconosciuti (nuovi). Se l'opzione è attivata, è possibile impostare il grado di rigidità dell'euristica. Questa opzione è attivata di default.

Livello di rilevamento basso

Se l'opzione è attivata, viene riconosciuto un numero inferiore di malware sconosciuti e il rischio di possibili rilevamenti di errore è limitato.

Livello di rilevamento medio

Questa impostazione è attivata di default, se è stata scelta l'applicazione di questa euristica.

Livello di riconoscimento elevato

Se l'opzione è attivata, viene riconosciuto un numero significativamente maggiore di malware sconosciuti, ma possono verificarsi messaggi di errore.

13.2.2 ProActiv

L'impiego di Avira AntiVir ProActiv consente di proteggere il computer da minacce nuove e sconosciute per le quali non esistono ancora definizioni di virus né euristiche. La tecnologia ProActiv è integrata nel componente Guard e consente di osservare e analizzare le azioni dei programmi. Nel comportamento dei programmi vengono ricercati modelli di azioni tipici dei malware: tipo e svolgimento dell'azione. Se un programma presenta un comportamento tipico di un malware, viene considerato e notificato come un rilevamento di virus : è possibile bloccare l'esecuzione del programma oppure ignorare il messaggio e proseguire. È possibile classificare il programma come affidabile e aggiungerlo così al filtro delle applicazioni dei programmi consentiti. È possibile inoltre aggiungere il programma al filtro delle applicazioni dei programmi da bloccare indicando *Blocca sempre*.

Per rilevare i comportamenti sospetti, il componente ProActiv utilizza set di regole che sono state sviluppate dal Centro Ricerca Malware Avira. Tali set di regole sono alimentati dalle banche dati di Avira GmbH. Per la raccolta delle informazioni nelle banche dati Avira, Avira AntiVir ProActiv invia informazioni relative a programmi sospetti notificati. È possibile disattivare l'inoltro dei dati alle banche dati di Avira.

Suggerimenti
La tecnologia ProActiv non è ancora disponibile per i sistemi a 64 bit! In Windows 2000 non è presente il supporto per il componente ProActiv.

Generale

Attiva Avira AntiVir ProActiv

Se l'opzione è attivata, i programmi presenti sul computer vengono monitorati alla ricerca di azioni sospette. Se viene rilevato un comportamento tipico di un malware, si riceve un messaggio. È possibile bloccare il programma oppure proseguire con la sua esecuzione con "*Ignora*". Dal monitoraggio sono esclusi: i programmi classificati come affidabili, i programmi affidabili e firmati che sono contenuti di default nel filtro delle applicazioni consentite, tutti i programmi che sono stati aggiunti dall'utente al filtro delle applicazioni dei programmi consentiti.

Migliorare la sicurezza del proprio computer partecipando alla community AntiVir ProActiv

Se l'opzione è attivata, Avira AntiVir ProActiv invia i dati relativi ai programmi sospetti e in alcuni casi file di programma sospetti (file eseguibili) al Centro Ricerca Malware Avira per una verifica avanzata online. Una volta valutati, i dati confluiscono nei set di regole dell'analisi del comportamento ProActiv. In questo modo si prende parte alla community di Avira ProActiv e si fornisce il proprio contributo al continuo miglioramento e al perfezionamento della tecnologia di sicurezza ProActiv. Se l'opzione è disattivata non vengono inviati dati. Questo non influisce sulla funzionalità di ProActiv.

Per ulteriori informazioni, fare clic qui.

Mediante il link si accede a un sito Internet attraverso il quale si ricevono informazioni dettagliate della verifica avanzata online. I dati completi inviati da una verifica avanzata online sono disponibili sul sito Internet.

13.2.2.1. Filtro di applicazione: Applicazioni da bloccare

In *Filtro delle applicazioni: applicazioni da bloccare* è possibile inserire applicazioni classificate come dannose e che devono essere bloccate di default da Avira AntiVir ProActiv. Le applicazioni inserite non possono essere eseguite sul computer. Con l'opzione *Blocca sempre questo programma*, è possibile aggiungere programmi al filtro delle applicazioni da bloccare anche attraverso le comunicazioni del Guard relative a un comportamento sospetto da parte di un programma .

Applicazioni da bloccare

Applicazioni

Nell'elenco sono riportate tutte le applicazioni classificate come dannose e che sono state aggiunte dall'utente durante la configurazione o derivanti dai messaggi del componente ProActiv. Tali applicazioni vengono bloccate da Avira AntiVir ProActiv e non possono essere eseguite sul sistema. Ogni volta che viene avviato un programma da bloccare, compare un messaggio del sistema operativo. Le applicazioni da bloccare vengono identificate da Avira AntiVir ProActiv in base al percorso indicato e al nome del file e bloccate indipendentemente dal contenuto.

Campo

Immettere in questo campo l'applicazione da bloccare. Per identificare l'applicazione, è necessario inserire il percorso completo e il nome del file con la relativa estensione. Il percorso indicato deve contenere il drive in cui si trova l'applicazione, oppure iniziare con una variabile d'ambiente.

Il pulsante apre una finestra nella quale si ha la possibilità di selezionare l'applicazione da bloccare.

Aggiungi

Con il pulsante "**Aggiungi"**, è possibile accettare l'applicazione indicata nel campo nell'elenco delle applicazioni da bloccare.

Suggerimenti
Non è possibile aggiungere le applicazioni necessarie al funzionamento del sistema operativo.

Elimina

Con il pulsante "**Elimina"**, è possibile rimuovere un'applicazione selezionata dall'elenco delle applicazioni da bloccare.

13.2.2.2. Filtro di applicazione: Applicazioni consentite

In *Filtro delle applicazioni: applicazioni consentite* sono elencate le applicazioni escluse dal monitoraggio del componente ProActiv: i programmi firmati che sono classificati come affidabili e sono contenuti di default nell'elenco, tutte le applicazioni classificate come affidabili dall'utente e inserite nel filtro delle applicazioni: nella configurazione è possibile aggiungere delle applicazioni all'elenco delle applicazioni consentite. È inoltre possibile aggiungere delle applicazioni segnalate nelle comunicazioni del Guard relative a un comportamento sospetto da parte di un programma, attivando l'opzione nei messaggi del Guard **Programma attendibile**.

Applicazioni da escludere

Applicazioni

L'elenco contiene le applicazioni escluse dal monitoraggio del componente ProActiv. Nelle impostazioni di default dopo l'installazione, l'elenco contiene applicazioni firmate di produttori attendibili. È possibile inserire applicazioni classificate come attendibili mediante la configurazione o i messaggi del Guard. Il componente ProActiv identifica le applicazioni in base al percorso, al nome del file e al contenuto. La verifica dei contenuti è utile poiché a un programma possono essere aggiunti codici dannosi in un secondo momento, in seguito a modifiche come gli aggiornamenti. Con la modalità indicata è possibile stabilire se deve essere eseguita una verifica del contenuto: Con la modalità "*Contenuto*", vengono verificate le modifiche del contenuto nei file delle applicazioni indicate con percorso e nome prima che vengano escluse dal monitoraggio mediante il componente ProActiv. Nel caso di una modifica del contenuto del file, l'applicazione viene nuovamente monitorata dal componente ProActiv. Con la modalità "*Percorso*" non avviene alcuna verifica del contenuto prima che l'applicazione venga esclusa dal monitoraggio mediante Guard. Per cambiare la modalità di esclusione, fare clic sulla modalità indicata.

Attenzione
Utilizzare la modalità *Percorso* solo in casi eccezionali. In seguito a un aggiornamento, è possibile che a un'applicazione vengano aggiunti codici dannosi. L'applicazione che originariamente era innocua, ora è un malware.

Suggerimenti
Alcune applicazioni affidabili, ad esempio tutti i componenti applicativi del programma AntiVir, sono esclusi di default dal monitoraggio mediante ProActiv, tuttavia non sono riportati nell'elenco.

Campo

Inserire in questo campo l'applicazione che si intende escludere dal monitoraggio mediante il componente ProActiv. Per identificare l'applicazione, è necessario inserire il percorso completo e il nome del file con la relativa estensione. Il percorso indicato deve contenere il drive in cui si trova l'applicazione, oppure iniziare con una variabile d'ambiente.

Il pulsante apre una finestra nella quale si ha la possibilità di selezionare l'applicazione da escludere.

Aggiungi

Con il pulsante "**Aggiungi**", è possibile accettare l'applicazione indicata nel campo nell'elenco delle applicazioni da escludere.

Elimina

Con il pulsante "**Elimina"**, è possibile rimuovere un'applicazione selezionata dall'elenco delle applicazioni da escludere.

13.2.3 Report

Guard possiede una funzione di log molto vasta che può fornire all'utente o all'amministratore informazioni esatte sulla modalità di un rilevamento.

Funzione di log

In questo gruppo viene definita la portata contenutistica del file di report.

Disabilitato

Se l'opzione è attivata, il Guard non crea alcun protocollo.
In casi eccezionali si può rinunciare alla funzione di report, solo se si eseguono test con molti virus o programmi indesiderati.

Standard

Se l'opzione è attivata, il Guard registra informazioni importanti (su rilevamenti, avvisi ed errori) nel file di report, mentre le informazioni meno importanti vengono ignorate per maggiore chiarezza. Questa opzione è attivata di default.

Avanzato

Se l'opzione è attivata, il Guard registra nel file di report anche le informazioni meno importanti.

Completo

Se l'opzione è attivata, il Guard registra tutte le informazioni - anche quelle relative alla dimensione del file, al tipo, alla data, ecc. - nel file di report.

Limitazioni del file di report

Limita la dimensione a n MB

Se l'opzione è attivata, il file di report può essere limitato a una determinata dimensione; valori possibili: da 1 a 100 MB. Con la limitazione del file di report si introduce un intervallo di circa 50 kilobyte per non sovraccaricare il processore. Se la dimensione del file di report supera la dimensione indicata di 50 kilobyte, vengono automaticamente eliminate le voci meno recenti fin quando si raggiunge una dimensione inferiore a 50 kilobyte.

Backup file report prima della limitazione

Se l'opzione è attivata il file del report viene salvato prima dell'abbreviazione.

Scrivi la configurazione nel file di report

Se l'opzione è attivata, la configurazione utilizzata della scansione in tempo reale viene riportata nel file di report.

Suggerimenti
Se non sono state specificate limitazioni per i file di report, viene creato un nuovo file di report quando questo raggiunge le dimensioni di 100 MB. Viene creato un backup del report di dati precedente. Vengono mantenuti fino a tre backup di report di dati precedenti. Vengono eliminati di volta in volta i backup meno recenti.

13.3 MailGuard

La rubrica MailGuard della configurazione è dedicata alla configurazione di MailGuard.

13.3.1 Cerca

MailGuard viene utilizzato per verificare la presenza di virus, malware e spam nelle email in ingresso. Nelle email in uscita, MailGuard verifica la presenza di virus e malware. Le email in uscita, inviate da un Bot sconosciuto per la diffusione di spam sul computer dell'utente, possono essere bloccate da MailGuard.

Cerca

Attiva MailGuard

Se l'opzione è attivata, il traffico di email viene sottoposto a controlli tramite MailGuard. MailGuard è un server proxy che controlla il traffico di dati fra il server email utilizzato e il programma email client sul sistema: Nell'impostazione di default, vengono ricercati malware nelle email in entrata. Se l'opzione è disattivata, il servizio di MailGuard rimane attivo, tuttavia, il monitoraggio tramite MailGuard è disattivato.

Scansiona email in entrata

Se l'opzione è attivata, nelle email in entrata viene verificata la presenza di virus, malware e spam . MailGuard supporta i protocolli POP3 e IMAP. Attivare l'account di posta in entrata, utilizzato dal client email dell'utente per ricevere le email, per il monitoraggio mediante MailGuard.

Controlla account POP3

Se l'opzione è attivata, gli account POP3 vengono monitorati alla porte in ingresso.

Porte controllate

Immettere nel campo la porta utilizzata per la posta in ingresso dal protocollo POP3. Più porte vengono indicate separate da una virgola.

Standard

Il pulsante consente di reimpostare le porte indicate sulla porta standard di POP3.

Controlla account IMAP

Se l'opzione è attivata, gli account IMAP vengono monitorati alla porte in ingresso.

Porte controllate

Immettere nel campo la porta utilizzata dal protocollo IMAP. Più porte vengono indicate separate da una virgola.

Standard

Il pulsante consente di reimpostare le porte indicate sulla porta standard di IMAP.

Scansiona email in uscita (SMTP)

Se l'opzione è attivata, nelle email in uscita viene verificata la presenza di virus e malware. Le email inviate da Bot sconosciuti per la diffusione di spam vengono bloccate.

Porte controllate

Immettere nel campo la porta utilizzata per la posta in uscita dal protocollo SMTP. Più porte vengono indicate separate da una virgola.

Standard

Il pulsante consente di reimpostare le porte indicate sulla porta standard di SMTP.

Suggerimenti
Per verificare le porte e i protocolli utilizzati, richiamare le proprietà degli account di posta elettronica nel programma email client utilizzato. Vengono principalmente utilizzate porte standard.

13.3.1.1. Azione per i rilevamenti

Questa rubrica di configurazione contiene le impostazioni delle azioni da intraprendere quando MailGuard rileva un virus o un programma indesiderato in un'email o in un allegato.

Suggerimenti
Le azioni definite qui vengono eseguite sia in caso di rilevamento di un virus nelle email in ingresso che nelle email in uscita.

Azione per i rilevamenti

Interattivo

Se l'opzione è attivata, in caso di rilevamento di un virus o di un programma indesiderato in un'email o in un allegato appare una finestra di dialogo nella quale si può selezionare come procedere con l'email o con l'allegato infetto. Questa opzione è attivata di default.

Visualizza barra di progressione

Se l'opzione è attivata, durante il download delle email MailGuard mostra una barra di progressione. É possibile attivare questa opzione è possibile solo se è stata selezionata l'opzione **Interattivo**.

Automatico

Se l'opzione è attivata, non viene più segnalato il rilevamento di un virus o di un programma indesiderato. MailGuard reagisce conformemente alle impostazioni effettuate dall'utente in questa sezione.

Azione primaria

L'azione primaria è l'azione che viene eseguita quando MailGuard rileva un virus o un programma indesiderato in un'email. Se è stata selezionata l'opzione "**Ignora email"** in "**Allegati infetti"**, è possibile scegliere come procedere in caso di un rilevamento in un allegato.

elimina email

Se l'opzione è attivata, l'email infetta viene automaticamente eliminata in caso di rilevamento di un virus o di un programma indesiderato. Il corpo dell'email (body) viene sostituito dal testo standard indicato di seguito. Lo stesso vale per gli allegati (Attachments); anche questi ultimi vengono sostituiti da un testo standard.

Isola email

Se l'opzione è attivata, l'email completa, inclusi gli allegati, viene collocata in Quarantena in caso di rilevamento di virus e programmi indesiderati. Successivamente - se lo si desidera - può essere ripristinata. Le email infette vengono eliminate. Il corpo dell'email (body) viene sostituito dal testo standard indicato di seguito. Lo stesso vale per gli allegati (Attachments); anche questi ultimi vengono sostituiti da un testo standard.

ignora email

Se l'opzione è attivata, l'email infetta viene ignorata nonostante il rilevamento di un virus o di un programma indesiderato. Si ha tuttavia la possibilità di decidere come procedere con un allegato infetto:

Allegati infetti

L'opzione "**Allegati infetti"** è selezionabile solo se in "**Azione primaria"** è stata selezionata l'impostazione "**Ignora email"**. Con questa opzione si può decidere come procedere in caso di rilevamento in un allegato.

elimina

Se l'opzione è attivata, in caso di rilevamento di un virus o di un programma indesiderato l'allegato infetto viene eliminato e sostituito con un Testo standard.

isola

Se l'opzione è attivata, l'allegato infetto viene collocato in Quarantena e infine eliminato (sostituito con un testo standard). Successivamente - se lo si desidera - l'allegato può essere ripristinato.

ignora

Se l'opzione è attivata, l'allegato infetto viene ignorato e inoltrato nonostante il rilevamento di un virus o di un programma indesiderato.

Attenzione
Se si seleziona questa opzione non si usufruisce di alcuna protezione da parte di MailGuard contro virus e programmi indesiderati. Effettuare questa scelta solo se si è sicuri di quello che si sta facendo. Disattivare l'anteprima nel programma email, non aprire mai gli allegati facendo doppio clic!

13.3.1.2. Altre azioni

Questa rubrica di configurazione contiene ulteriori impostazioni relative alle azioni da intraprendere quando MailGuard rileva un virus o un programma indesiderato in un'email o in un allegato.

Suggerimenti
Le azioni qui impostate vengono eseguite solo se viene rilevato un virus nelle email in ingresso.

Testo standard per email eliminate e spostate

Il testo in questo campo viene sostituito all'email infetta come notifica nel messaggio. Tale messaggio è modificabile. Può contenere un numero massimo di 500 caratteri.

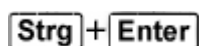
Per la formattazione si possono utilizzare le seguenti combinazioni di tasti:

Standard

Il pulsante inserisce un testo standard predefinito nel campo.

Testo standard per allegati eliminati e spostati

Il testo in questo campo viene sostituito all'allegato infetto come notifica nell'email. Tale messaggio è modificabile. Può contenere un numero massimo di 500 caratteri.

Per la formattazione si possono utilizzare le seguenti combinazioni di tasti:

aggiunge un'interruzione di riga.

Standard

Il pulsante inserisce un testo standard predefinito nel campo.

13.3.1.3. Euristico

Questa rubrica di configurazione contiene le impostazioni per l'euristica del motore di ricerca.

I prodotti AntiVir contengono un'euristica molto efficace, che consente di riconoscere in modo proattivo malware sconosciuti, ovvero prima che venga creata una firma speciale dei virus contro il parassita e che venga inviato un aggiornamento della protezione antivirus. Il riconoscimento dei virus avviene attraverso un'approfondita analisi e indagine del relativo codice in base alle funzioni tipiche dei malware. Se il codice esaminato corrisponde a tali caratteristiche tipiche viene segnalato come sospetto. Ciò non significa necessariamente che il codice indichi effettivamente la presenza di un malware; potrebbe trattarsi anche di messaggi di errore. La decisione su come procedere con il codice spetta all'utente stesso, ad esempio sulla base delle sue conoscenze relativamente all'attendibilità della fonte che contiene il codice segnalato.

Macrovirus euristico

Attiva macrovirus euristico

Il prodotto AntiVir acquistato contiene un macrovirus euristico molto efficace. Se l'opzione è attivata, in caso di riparazione possibile tutte le macro del documento infetto vengono eliminate, in alternativa i documenti sospetti vengono solo segnalati, l'utente riceverà quindi un avviso. Questa impostazione è attivata di default e viene consigliata.

Advanced Heuristic Analysis and Detection (AHeAD)

Attiva AHeAD

Il programma AntiVir contiene, grazie alla tecnologia AntiVir AHeAD, un'euristica molto efficace, in grado di riconoscere anche malware sconosciuti (nuovi). Se l'opzione è attivata, è possibile impostare il grado di rigidità dell'euristica. Questa opzione è attivata di default.

Livello di rilevamento basso

Se l'opzione è attivata, viene riconosciuto un numero inferiore di malware sconosciuti e il rischio di possibili rilevamenti di errore è limitato.

Livello di rilevamento medio

Questa opzione è attivata di default, se è stata scelta l'applicazione di questa euristica. Questa impostazione è attivata di default e viene consigliata.

Livello di riconoscimento elevato

Se l'opzione è attivata, viene riconosciuto un numero significativamente maggiore di malware sconosciuti, ma possono verificarsi messaggi di errore.

13.3.1.4. AntiBot

La funzione AntiBot di MailGuard consente di evitare che il computer venga sfruttato per la diffusione di email di spam all'interno di una cosiddetta Bot-Net: per la diffusione di spam tramite una Bot-Net, di norma un aggressore infetta diversi computer con un bot, che si collega a un server IRC, utilizza un canale specifico e qui attende il comando di invio delle email di spam. Per differenziare le email di spam di un bot sconosciuto da quelle dell'utente, MailGuard verifica se il server SMTP utilizzato e il mittente dell'email in uscita si trovano nell'elenco dei server e dei mittenti autorizzati. In caso contrario, l'email in uscita viene bloccata, ovvero non viene inviata. L'email bloccata viene segnalata in una finestra di dialogo.

Suggerimenti
La funzione AntiBot può essere utilizzata solo se la scansione di MailGuard è attiva per le email in uscita (vedere l'opzione **Scansione email in uscita** in MailGuard :: Scansione).

Server consentiti

Tutti i server in questo elenco sono autorizzati da MailGuard all'invio di email: le email inviate a questi server **non** vengono bloccate da MailGuard. Se l'elenco non contiene alcun server, nelle email in uscita non viene verificato il server SMTP utilizzato. Se l'elenco contiene delle voci, MailGuard blocca le email inviate a un server SMTP che non è presente nell'elenco.

Campo

In questo campo vengono immessi il nome host e l'indirizzo IP del server SMTP utilizzato per l'invio delle email.

Suggerimenti
I dati relativi ai server SMTP utilizzati dal programma email per l'invio delle email sono riportati all'interno del programma email nei dati dell'account utente impostati.

Aggiungi

Il pulsante consente di aggiungere il server inserito nel campo all'elenco dei server autorizzati.

Elimina

Il pulsante elimina una voce selezionata dall'elenco dei server autorizzati. Questo pulsante non è attivo se non è selezionata alcuna voce.

Elimina tutti

Il pulsante elimina tutte le voci dell'elenco dei server autorizzati.

Mittenti consentiti

Tutti i mittenti in questo elenco sono autorizzati da MailGuard all'invio di email: le email inviate da questi indirizzi email **non** vengono bloccate da MailGuard. Se l'elenco non contiene alcun mittente, nelle email in uscita non viene verificato l'indirizzo email del mittente. Se l'elenco contiene delle voci, MailGuard blocca le email inviate da mittenti non presenti nell'elenco.

Campo

In questo campo immettere gli indirizzi email dei mittenti.

Aggiungi

Il pulsante consente di aggiungere il mittente inserito nel campo all'elenco dei mittenti autorizzati.

Elimina

Il pulsante elimina una voce selezionata dall'elenco dei mittenti autorizzati. Questo pulsante non è attivo se non è selezionata alcuna voce.

Elimina tutti

Il pulsante elimina tutte le voci dall'elenco dei mittenti autorizzati.

13.3.2 Generale

13.3.2.1. Eccezioni

Indirizzi email non verificati

Questa tabella mostra l'elenco di indirizzi email esclusi dalla scansione di AntiVir MailGuard (white list).

Suggerimenti
L'elenco delle eccezioni viene utilizzato da MailGuard esclusivamente per le email in ingresso.

Stato

Simbolo	Descrizione
	Questo indirizzo email non viene più sottoposto a controlli antispam.
	Questo indirizzo email non viene più sottoposto a controlli per malware.
	Questo indirizzo email non viene più sottoposto a controlli antispam e malware.

Indirizzo email

Indirizzo email che non deve più essere scansionato.

Malware

Se l'opzione è attivata, l'indirizzo email non viene più sottoposto a controlli per malware.

Spam

Se l'opzione è attivata, l'indirizzo email non viene più sottoposto a controlli antispam.

in alto

Questo pulsante consente di spostare un indirizzo email selezionato di una posizione verso l'alto. Il pulsante non è attivo se non è selezionata alcuna voce o se l'indirizzo contrassegnato si trova già nella prima posizione dell'elenco.

in basso

Questo pulsante consente di spostare un indirizzo email selezionato di una posizione verso il basso. Il pulsante non è attivo se non è selezionata alcuna voce o se l'indirizzo contrassegnato si trova già nell'ultima posizione dell'elenco.

Campo

Inserire in questo campo gli indirizzi email che si desidera aggiungere all'elenco degli indirizzi email da non controllare. L'indirizzo email non verrà più controllato da MailGuard in futuro - in base alle impostazioni dell'utente.

Suggerimenti
Quando si immettono indirizzi email si possono utilizzare wildcard: wildcard * per il numero di caratteri desiderato e wildcard **?** per un solo carattere. Tuttavia le wildcard possono essere utilizzate solo per gli indirizzi email che non devono essere verificati per lo spam. Se si tenta di escludere dalla verifica del malware un indirizzo con metacaratteri viene visualizzato un messaggio di errore, mentre è stata selezionata la casella di controllo **Malware** nell'elenco delle esclusioni. Nell'immettere indirizzi con wildcard assicurarsi che alla sequenza indicata corrisponda la struttura di un indirizzo email (*@*.*).

Attenzione
Nell'utilizzo di wildcard, considerare gli esempi riportati. Impostare esclusivamente wildcard mirate e verificare con attenzione gli indirizzi email da inserire nella white list per lo spam con l'immissione di wildcard.

Esempi: utilizzo di wildcard negli indirizzi email (white list per lo spam)

- `virus@avira.* /` = raggruppa tutte le email con questo indirizzo e con il dominio di livello superiore desiderato: virus@avira.de, virus@avira.com, virus@avira.net,...
- `*@avira.com` = raggruppa tutte le email inviate dal dominio **avira.com**: info@avira.com, virus@avira.com, kontakt@avira.com, mitarbeiter@avira.com
- `info@*.com` = raggruppa tutti gli indirizzi email con il dominio di livello superiore **com** e l'indirizzo **info**: il dominio di secondo livello è libero: info@name1.com, info@name2.com,...

Aggiungi

Con il pulsante è possibile aggiungere alla lista degli indirizzi email da non verificare un indirizzo email indicato nel campo.

Elimina

Il pulsante elimina un indirizzo email contrassegnato dall'elenco.

Importa rubrica di Outlook

Il pulsante consente di importare indirizzi email dalla rubrica del programma di posta elettronica MS Outlook nell'elenco delle eccezioni. Negli indirizzi email importati non viene verificata la presenza di spam.

Importa rubrica di Outlook Express

Il pulsante consente di importare gli indirizzi email dalla rubrica del programma di posta elettronica MS Outlook Express nell'elenco delle eccezioni. Negli indirizzi email importati non viene verificata la presenza di spam.

13.3.2.2. Memoria temporanea

Memoria temporanea

La memoria temporanea di MailGuard contiene i dati relativi alle email scansionate che vengono visualizzati nella statistica del Control Center in MailGuard. Inoltre, le copie delle email in entrata possono essere archiviate nella memoria temporanea. Le email vengono utilizzate per le funzioni di training (email buona - utilizza per training, spam - utilizza per training) del modulo AntiSpam.

Suggerimenti
Per salvare le email in entrata nella memoria temporanea, il modulo AntiSpam deve essere attivato.

Numero massimo di email da memorizzare nella memoria temporanea

In questo campo viene indicato il numero massimo di email che MailGuard conserva nella memoria temporanea. Vengono eliminate le email più vecchie.

Durata massima della memorizzazione di un'email in giorni

In questo campo viene inserita la durata massima della memorizzazione di un'email in giorni. Dopo questo tempo, l'email viene eliminata dalla memoria temporanea.

Svuota memoria temp.

Facendo clic sul pulsante vengono eliminate le email che vengono conservate nella memoria temporanea.

13.3.2.3. MailGuard

AntiSpam

AntiVir MailGuard scansiona le email alla ricerca di virus e programmi indesiderati. Inoltre offre una protezione affidabile contro le email di spam.

AntiSpam

Attiva modulo AntiSpam

Se l'opzione è attivata, la funzione antispam di MailGuard viene attivata.

Seleziona oggetto email

Se l'opzione è attivata, quando viene rilevata un'email di spam viene aggiunta una nota all'oggetto originario dell'email.

Semplice

Viene aggiunta una nota all'oggetto di un'email di spam o di phishing: [SPAM] o [Phishing]. Questa opzione è attivata di default.

Dettagliato

All'oggetto di un'email spam o di phishing viene aggiunta una nota sulla probabilità che si tratti di spam.

Registra

Se l'opzione è attivata, MailGuard crea uno speciale file di report AntiSpam.

Utilizza black list in tempo reale

Se l'opzione è attivata, viene esaminata in tempo reale una cosiddetta "black list" che mette a disposizione informazioni aggiuntive per classificare come spam le email di origine dubbia.

Timeout: n secondo(i)

Se le informazioni di una blacklist non è disponibile dopo n secondi, viene interrotto il tentativo di richiamare la blacklist.

Elimina la banca dati training

Facendo clic sul pulsante vengono eliminate le banche dati training.

Aggiungi automaticamente alla white list il destinatario della email in uscita

Se l'opzione è attivata, gli indirizzi dei destinatari delle email in uscita vengono inseriti automaticamente nella whitelist dello spam (elenco di email che non vengono verificate per lo spam in **MailGuard :: Generale :: Eccezioni**). Le email in ingresso che provengono da indirizzi della white list dello spam non vengono verificate per lo spam. Viene comunque verificata la presenza di virus e malware. Questa opzione è disattivata di default.

Suggerimenti
Questa opzione può essere attivata solo se la scansione di MailGuard è attiva per le email in uscita (vedere l'opzione **Scansione email in uscita** in MailGuard :: Scansione).

13.3.2.4. Piè di pagina

In *Piè di pagina* è possibile configurare un piè di pagina che verrà visualizzato nelle email inviate dall'utente. Il presupposto per questa funzione è l'attivazione del controllo MailGuard per le email in uscita (vedere l'opzione *Scansione email in uscita (SMTP)* in Configurazione::MailGuard::Scansione). È possibile utilizzare il piè di pagina definito di AntiVir MailGuard con il quale si conferma che l'email inviata è stata controllata da un programma antivirus. È anche possibile immettere un testo per un piè di pagina personalizzato. Se vengono utilizzate entrambe le opzioni come piè di pagina, il testo personalizzato viene anteposto al piè di pagina di AntiVir MailGuard.

Piè di pagina nelle email da inviare

Allega piè di pagina AntiVir MailGuard

Se l'opzione è attivata, viene visualizzato il piè di pagina AntiVir MailGuard nel testo del messaggio delle email inviate. Con il piè di pagina AntiVir MailGuard si conferma che l'email inviata è stata controllata da AntiVir MailGuard per virus e programmi indesiderati e che non proviene da un bot sconosciuto. Il piè di pagina AntiVir MailGuard contiene il testo seguente: "Scansionato con AntiVir MailGuard [versione del prodotto] [abbreviazione del nome e numero versione del motore di ricerca] [abbreviazione del nome e numero versione del file di definizione dei virus]".

Allega questo piè di pagina

Se l'opzione è attivata, il testo indicato nel campo viene visualizzato come piè di pagina.

Campo

In questo campo è possibile immettere un testo che viene visualizzato come piè di pagina nelle email inviate.

13.3.3 Report

MailGuard possiede una funzione di log molto vasta che può fornire all'utente o all'amministratore informazioni esatte sulla modalità di un rilevamento.

Funzione di log

In questo gruppo viene definita la portata contenutistica del file di report.

Disabilitato

Se l'opzione è attivata, MailGuard non crea alcun protocollo.
In casi eccezionali si può rinunciare alla funzione di report, solo se si eseguono test con molti virus o programmi indesiderati.

Standard

Se l'opzione è attivata, MailGuard registra informazioni importanti (su rilevamenti, avvisi ed errori) nel file di report, mentre le informazioni meno importanti vengono ignorate per maggiore chiarezza. Questa opzione è attivata di default.

Avanzato

Se l'opzione è attivata, MailGuard registra nel file di report anche le informazioni meno importanti.

Completo

Se l'opzione è attivata, MailGuard registra nel file di report tutte le informazioni.

Limitazioni del file di report

Limita la dimensione a n MB

Se l'opzione è attivata, il file di report può essere limitato a una determinata dimensione; valori possibili: da 1 a 100 MB. Con la limitazione del file di report si introduce un intervallo di circa 50 kilobyte per non sovraccaricare il processore. Se la dimensione del file di report supera la dimensione indicata di 50 kilobyte, vengono automaticamente eliminate le voci meno recenti fin quando si raggiunge una dimensione inferiore a 50 kilobyte.

Backup file report prima della limitazione

Se l'opzione è attivata il file del report viene salvato prima dell'abbreviazione.

Scrivi la configurazione nel file di report

Se l'opzione è attivata, la configurazione di MailGuard utilizzata viene scritta nel file di report.

Suggerimenti
Se non sono state specificate limitazioni per i file di report, viene creato un nuovo file di report quando questo raggiunge le dimensioni di 100 MB. Viene creato un backup del report di dati precedente. Vengono mantenuti fino a tre backup di report di dati precedenti. Vengono eliminati di volta in volta i backup meno recenti.

13.4 FireWall

La rubrica FireWall della configurazione è dedicata alla configurazione del componente FireWall di Avira.

13.4.1 Regole adattatore

Il FireWall di Avira considera adattatore qualsivoglia unità hardware simulata da un software (ad esempio Miniport, Bridge Connection, ecc.) o qualsivoglia unità hardware (ad esempio una scheda di rete).

Il FireWall di Avira visualizza le regole adattatore per tutti gli adattatori presenti sul computer per i quali è installato un driver.

Una regola adattatore predefinita dipende dal livello di sicurezza. Tramite la rubrica Protezione online :: Con il Firewall del Control Center è possibile modificare il livello di sicurezza o adeguare le regole adattatore alle proprie esigenze. Se le regole adattatore sono state adeguate alle proprie esigenze, nella rubrica Firewall del Control Center, nella sezione Livello di sicurezza, il cursore sarà posizionato sul profilo utente.

Suggerimenti
L'impostazione standard del livello di sicurezza per tutte le regole predefinite del Firewall di Avira è **medio**.

Protocollo ICMP

L'Internet Control Message Protocol (ICMP) serve allo scambio di informazioni o comunicazione di errori nelle reti. Il protocollo viene utilizzato anche per le comunicazioni sullo status per mezzo di Ping o Tracert.
Con questa regola è possibile definire le tipologie ICMP in entrata e in uscita che dovrebbero essere bloccate, fissare i parametri per il flooding e definire il comportamento da tenere in caso di pacchetti ICMP frammentati. Questa regola serve a evitare i cosiddetti attacchi ICPM Flood, che potrebbero comportare un carico o un sovraccarico del processore del computer attaccato, poiché risponde a ogni pacchetto.

Regole predefinite per il protocollo ICMP

Impostazione: Livello basso	Impostazione: Livello medio	Impostazione: Livello elevato
Tipi in entrata bloccati: **nessun tipo**. Tipi in uscita bloccati: **nessun tipo**. Supporre un flooding se il ritardo tra i pacchetti è inferiore a **50** millisecondi. **Rifiuta** pacchetti ICMP frammentati.	La stessa regola applicata con l'impostazione livello basso.	Tipi in entrata bloccati: **diversi tipi**. Tipi in uscita bloccati: **diversi tipi**. Supporre un flooding se il ritardo tra i pacchetti è inferiore a **50** millisecondi. **Rifiuta** pacchetti ICMP frammentati.

Tipi in entrata bloccati: nessun tipo/diversi tipi

Facendo clic con il mouse sul link si apre un elenco contenente i tipi di pacchetti ICMP. Da questi elenchi è possibile selezionare i tipi ICMP che si desidera bloccare.

Tipi in uscita bloccati: nessun tipo/diversi tipi

Facendo clic con il mouse sul link si apre un elenco contenente i tipi di pacchetti ICMP. Dall'elenco è possibile selezionare le tipologie di notifiche ICMP che si desidera bloccare.

Flooding

Facendo clic con il mouse sul link si apre una finestra di dialogo in cui è possibile inserire il valore massimo per il ritardo ICMP consentito.

Pacchetti ICMP frammentati

Facendo clic con il mouse sul link si ha la possibilità di scegliere se accettare o rifiutare i pacchetti ICMP frammentati.

Port-Scan TCP

Con questa regola è possibile definire quando il FireWall deve supporre un Port-Scan TCP e come comportarsi in un caso del genere. Questa regola serve a evitare i cosiddetti attacchi Port-Scan TCP mediante i quali si creano porte aperte sul computer. Gli attacchi di questo tipo vengono principalmente usati per sfruttare i punti deboli del proprio computer che serviranno poi per eseguire attacchi pericolosi.

Regole predefinite per il Port-Scan TCP

Impostazione: Livello basso	**Impostazione: Livello medio**	**Impostazione: Livello elevato**
Supporre un Port-Scan TCP in corso quando **50** o più porte vengono scansionate in **5000** millisecondi. In caso di un Port-Scan TCP, **scrivere nel file di report** l'indirizzo IP dell'aggressore e **aggiungere** alle regole per bloccare l'attacco.	Supporre un Port-Scan TCP in corso quando **50** o più porte vengono scansionate in **5000** millisecondi. In caso di un Port-Scan TCP, **scrivere nel file di report** l'indirizzo IP dell'aggressore e **aggiungere** alle regole per bloccare l'attacco.	La stessa regola applicata con l'impostazione livello medio.

Porte

Facendo clic con il mouse sul link si apre una finestra di dialogo nella quale è possibile immettere il numero di porte che devono essere scansionate, in modo da escludere un Port-Scan TCP.

Finestra temporale del Port-Scan

Facendo clic con il mouse sul link si apre una finestra di dialogo nella quale è possibile immettere l'intervallo di tempo in cui un determinato numero di porte dovrebbe essere scansionato, in modo da escludere un Port-Scan TCP.

File di report

Facendo clic con il mouse su questo link si ha la possibilità di decidere se scrivere o meno l'indirizzo IP dell'aggressore nel file di report.

Regola

Facendo clic con il mouse su questo link si ha la possibilità di decidere se aggiungere o meno la regola per il blocco dell'attacco Port-Scan TCP.

Port-Scan UDP

Con questa regola è possibile definire quando il FireWall deve supporre un Port-Scan UDP e come comportarsi in un caso del genere. Questa regola serve a evitare i cosiddetti attacchi Port-Scan UDP mediante i quali si creano porte aperte sul proprio computer. Gli attacchi di questo tipo vengono principalmente usati per sfruttare i punti deboli del proprio computer che serviranno poi per eseguire attacchi pericolosi.

Regole predefinite per il Port-Scan UDP

Impostazione: Livello basso	Impostazione: Livello medio	Impostazione: Livello elevato
Supporre un Port-Scan UDP in corso quando **50** o più porte vengono scansionate in **5000** millisecondi. In caso di un Port-Scan UDP, **scrivere nel file di report** l'indirizzo IP dell'aggressore e **non aggiungerlo** alle regole per bloccare l'attacco.	Supporre un Port-Scan UDP in corso quando **50** o più porte vengono scansionate in **5000** millisecondi. In caso di un Port-Scan TCP, **scrivere nel file di report** l'indirizzo IP dell'aggressore e **aggiungere** alle regole per bloccare l'attacco.	La stessa regola applicata con l'impostazione livello medio.

Porte

Facendo clic con il mouse sul link si apre una finestra di dialogo nella quale è possibile indicare il numero di porte che devono essere scansionate in modo da escludere un Port-Scan UDP.

Finestra temporale del Port-Scan

Facendo clic con il mouse sul link si apre una finestra di dialogo nella quale è possibile immettere l'intervallo di tempo in cui un determinato numero di porte dovrebbe essere scansionato, in modo da escludere un Port-Scan UDP.

File di report

Facendo clic con il mouse su questo link si ha la possibilità di decidere se scrivere o meno l'indirizzo IP dell'aggressore nel file di report.

Regola

Facendo clic con il mouse su questo link si ha la possibilità di decidere se aggiungere o meno la regola per il blocco dell'attacco Port-Scan UDP.

13.4.1.1. Regole in entrata

Le regole in entrata servono a controllare lo scambio dati in entrata con il Firewall di Avira.

Suggerimenti
Dal momento che per filtrare un pacchetto vengono applicate le regole una dopo l'altra, la loro sequenza è di particolare importanza. Si prega di modificare la sequenza delle regole solo quando si è completamente sicuri del risultato che si otterrà.

Regole predefinite per il monitoraggio dello scambio dati TCP

Impostazione: Livello basso	Impostazione: Livello medio	Impostazione: Livello elevato
Lo scambio di dati in entrata non viene bloccato dal FireWall	– Consenti la connessione TCP esistente sulla	– Monitorare il traffico dati TCP consentito

di Avira.	porta 135 **Consenti** pacchetti TCP, dall'indirizzo **0.0.0.0** con maschera **0.0.0.0**, se la porta locale è **{135}** e la porta remota **{0-65535}**. Applica ai **pacchetti delle connessioni disponibili**. **Non scrivere nel file di report** se il pacchetto corrisponde alla regola. Esteso: rifiuta i pacchetti con i seguenti bytes **<vuoto>** con maschera **<vuoto>** all'offset **0**. – Rifiuta pacchetti TCP sulla porta 135 **rifiuta**pacchetti TCP dall'indirizzo **0.0.0.0** con maschera **0.0.0.0**, se la porta locale è **{135}** e la porta remota **{0-65535}**. Applica a **tutti i pacchetti**. **Non scrivere nel file di report** se il pacchetto corrisponde alla regola. Esteso: Rifiuta i pacchetti con i seguenti byte **<vuoto>** con maschera **<vuoto>**	**Consenti** pacchetti TCP, dall'indirizzo **0.0.0.0** con maschera **0.0.0.0**, se la porta locale è **{0-65535}** e la porta remota **{0-65535}**. Applica ai **pacchetti delle connessioni disponibili**. **Non scrivere nel file di report** se il pacchetto corrisponde alla regola. Esteso: rifiuta i pacchetti con i seguenti bytes **<vuoto>** con maschera **<vuoto>** all'offset **0**.

	all'offset **0**. – Monitoraggio del traffico dati conforme TCP **Consenti** pacchetti TCP, dall'indirizzo **0.0.0.0** con maschera **0.0.0.0**, se la porta locale è **{0-65535}** e la porta remota **{0-65535}**. Applica all'**inizio dello stabilimento di una connessione e ai pacchetti delle connessioni disponibili.** **Non scrivere nel file di report** se il pacchetto corrisponde alla regola. Esteso: rifiuta i pacchetti con i seguenti bytes **<vuoto>** con maschera **<vuoto>** all'offset **0**. – Rifiuta tutti i pacchetti TCP Rifiuta **i pacchetti TCP**, dall'indirizzo **0.0.0.0** con maschera **0.0.0.0**, se la porta locale è **{0-65535}** e la porta remota è **{0-65535}**. Applica a **tutti i pacchetti**. **Non scrivere nel file di report** se il pacchetto	

	corrisponde alla regola. Esteso: rifiuta i pacchetti con i seguenti bytes **<vuoto>** con maschera **<vuoto>** all'offset **0**.	

Consenti / rifiuta pacchetti TCP

Facendo clic con il mouse su questo link si ha la possibilità di decidere se consentire o rifiutare i pacchetti TCP.

Indirizzo IP

Facendo clic con il mouse su questo link si apre una finestra di dialogo nella quale è possibile inserire gli indirizzi IP desiderati.

Maschera IP

Facendo clic con il mouse su questo link si apre una finestra di dialogo nella quale è possibile inserire le maschere IP desiderate.

Porte locali

Facendo clic con il mouse su questo link si apre una finestra di dialogo nella quale è possibile inserire una o più porte locali e anche intere sezioni delle porte.

Porte remote

Facendo clic con il mouse sul link si apre una finestra di dialogo in cui è possibile inserire una o più porte remote desiderate e anche intere sezioni delle porte.

Metodi di applicazione

Facendo clic con il mouse sul link si ha la possibilità di utilizzare la regola sui pacchetti di connessioni disponibili all'inizio dello stabilimento della connessione e i pacchetti delle connessioni esistenti o su tutte le connessioni.

File di report

Facendo clic con il mouse sul link si ha la possibilità di decidere di scrivere o meno nel file di report se il pacchetto corrisponde alla regola.

L'opzione **Esteso** consente una filtrazione a causa del contenuto. È possibile così, ad esempio, rifiutare i pacchetti che contengono dati specifici con un offset preciso. Se non si desidera utilizzare questa opzione non selezionare alcun file o selezionare un file vuoto.

Filtrazione per contenuto: Dati

Facendo clic con il mouse sul link si apre una finestra di dialogo nella quale è possibile selezionare il file che contiene il buffer speciale.

Filtrazione per contenuto: maschera

Facendo clic con il mouse sul link si apre una finestra di dialogo nella quale è possibile selezionare la maschera speciale.

Filtrazione per contenuto: offset

Facendo clic con il mouse sul link si apre una finestra di dialogo nella quale è possibile inserire l'offset per la filtrazione di contenuti. L'offset viene calcolato dalla fine dell'header TCP.

Regole predefinite per il monitoraggio dello scambio dati UDP

Impostazione: Livello basso	Impostazione: Livello medio	Impostazione: Livello elevato
-	– Monitoraggio del traffico dati conforme UDP **Consenti** pacchetti UDP, dall'indirizzo **0.0.0.0** con maschera **0.0.0.0**, se la porta locale è **{0-65535}** e la porta remota **{0-65535}**. Applica la regola alle **porte aperte**. **Non scrivere nel file di report** se il pacchetto corrisponde alla regola. Esteso: rifiuta i pacchetti con i seguenti bytes **<vuoto>** con maschera **<vuoto>** all'offset **0**. – Rifiuta tutti i pacchetti UDP Rifiuta **i pacchetti UDP**, dall'indirizzo **0.0.0.0** con maschera **0.0.0.0**, se la porta locale è **{0-65535}** e la porta remota è **{0-65535}**. Applica a **tutte le porte**. **Non scrivere nel file di report** se il pacchetto corrisponde alla	Monitorare il traffico dati UDP consentito **Consenti** pacchetti UDP, dall'indirizzo **0.0.0.0** con maschera **0.0.0.0**, se la porta locale è **{0-65535}** e la porta remota è **{53, 67, 68, 123}**. Applica la regola alle **porte aperte**. **Non scrivere nel file di report** se il pacchetto corrisponde alla regola. Esteso: rifiuta i pacchetti con i seguenti bytes **<vuoto>** con maschera **<vuoto>** all'offset **0**.

		regola. Esteso: rifiuta i pacchetti con i seguenti bytes **<vuoto>** con maschera **<vuoto>** all'offset **0**.	

Consenti / rifiuta pacchetti UDP

Facendo clic con il mouse su questo link si ha la possibilità di decidere se consentire o rifiutare i pacchetti UDP.

Indirizzo IP

Facendo clic con il mouse su questo link si apre una finestra di dialogo nella quale è possibile inserire gli indirizzi IP desiderati.

Maschera IP

Facendo clic con il mouse su questo link si apre una finestra di dialogo nella quale è possibile inserire le maschere IP desiderate.

Porte locali

Facendo clic con il mouse su questo link si apre una finestra di dialogo nella quale è possibile inserire una o più porte locali e anche intere sezioni delle porte.

Porte remote

Facendo clic con il mouse sul link si apre una finestra di dialogo in cui è possibile inserire una o più porte remote desiderate e anche intere sezioni delle porte.

Metodi di applicazione

Facendo clic con il mouse sul link si ha la possibilità di decidere se si desidera applicare la regola a tutte le porte o solo alle porte aperte.

File di report

Facendo clic con il mouse sul link si ha la possibilità di decidere di scrivere o meno nel file di report se il pacchetto corrisponde alla regola.

L'opzione **Esteso** consente una filtrazione a causa del contenuto. È possibile così, ad esempio, rifiutare i pacchetti che contengono dati specifici con un offset preciso. Se non si desidera utilizzare questa opzione non selezionare alcun file o selezionare un file vuoto.

Filtrazione per contenuto: Dati

Facendo clic con il mouse sul link si apre una finestra di dialogo nella quale è possibile selezionare il file che contiene il buffer speciale.

Filtrazione per contenuto: maschera

Facendo clic con il mouse sul link si apre una finestra di dialogo nella quale è possibile selezionare la maschera speciale.

Filtrazione per contenuto: offset

Facendo clic con il mouse sul link si apre una finestra di dialogo nella quale è possibile inserire l'offset per la filtrazione di contenuti. L'offset viene calcolato dalla fine dell'header UDP.

Regole predefinite per il monitoraggio dello scambio dati ICMP

Impostazione: Livello basso	Impostazione: Livello medio	Impostazione: Livello elevato
-	– Non rifiutare pacchetti ICMP sulla base dell'indirizzo IP **Consenti** pacchetti ICMP dell'indirizzo **0.0.0.0** con maschera**0.0.0.0**. **Non scrivere nel file di report** se il pacchetto corrisponde alla regola. Esteso: rifiuta i pacchetti con i seguenti bytes **<vuoto>** con maschera **<vuoto>** all'offset **0**.	La stessa regola applicata con l'impostazione livello medio.

Consenti / rifiuta pacchetti ICMP

Facendo clic con il mouse su questo link si ha la possibilità di decidere se consentire o rifiutare i pacchetti ICMP.

Indirizzo IP

Facendo clic con il mouse su questo link si apre una finestra di dialogo nella quale è possibile inserire gli indirizzi IP desiderati.

Maschera IP

Facendo clic con il mouse su questo link si apre una finestra di dialogo nella quale è possibile inserire le maschere IP desiderate.

File di report

Facendo clic con il mouse sul link si ha la possibilità di decidere di scrivere o meno nel file di report se il pacchetto corrisponde alla regola.

L'opzione **Esteso** consente una filtrazione a causa del contenuto. È possibile così, ad esempio, rifiutare i pacchetti che contengono dati specifici con un offset preciso. Se non si desidera utilizzare questa opzione non selezionare alcun file o selezionare un file vuoto.

Filtrazione per contenuto: Dati

Facendo clic con il mouse sul link si apre una finestra di dialogo nella quale è possibile selezionare il file che contiene il buffer speciale.

Filtrazione per contenuto: maschera

Facendo clic con il mouse sul link si apre una finestra di dialogo nella quale è possibile selezionare la maschera speciale.

Filtrazione per contenuto: offset

Facendo clic con il mouse sul link si apre una finestra di dialogo nella quale è possibile inserire l'offset per la filtrazione di contenuti. L'offset viene calcolato dalla fine dell'header ICMP.

Regola predefinita per i pacchetti IP

Impostazione: Livello basso	Impostazione: Livello medio	Impostazione: Livello elevato
-	-	Rifiuta tutti i pacchetti IP Consenti **pacchetti IP** dall'indirizzo **0.0.0.0** con maschera **0.0.0.0**. **Non scrivere nel file di report** se il pacchetto corrisponde alla regola.

Consenti / rifiuta pacchetti IP

Facendo clic con il mouse su questo link si ha la possibilità di decidere se consentire o rifiutare i pacchetti IP speciali definiti.

Indirizzo IP

Facendo clic con il mouse su questo link si apre una finestra di dialogo nella quale è possibile inserire gli indirizzi IP desiderati.

Maschera IP

Facendo clic con il mouse su questo link si apre una finestra di dialogo nella quale è possibile inserire le maschere IP desiderate.

File di report

Facendo clic con il mouse sul link si ha la possibilità di decidere di scrivere o meno nel file di report se il pacchetto corrisponde alla regola.

Possibile regola per il monitoraggio di pacchetti IP sulla base dei protocolli IP

Pacchetti IP

Facendo clic con il mouse su questo link si ha la possibilità di decidere se consentire o rifiutare i pacchetti IP speciali definiti.

Indirizzo IP

Facendo clic con il mouse su questo link si apre una finestra di dialogo nella quale è possibile inserire gli indirizzi IP desiderati.

Maschera IP

Facendo clic con il mouse su questo link si apre una finestra di dialogo nella quale è possibile inserire le maschere IP desiderate.

Protocollo

Facendo clic con il mouse su questo link si apre una finestra di dialogo nella quale è possibile selezionare il protocollo IP desiderato.

File di report

Facendo clic con il mouse sul link si ha la possibilità di decidere di scrivere o meno nel file di report se il pacchetto corrisponde alla regola.

13.4.1.2. Regole in uscita

Le regole in uscita servono a controllare lo scambio dati in uscita con il FireWall di Avira. È possibile definire una regola in uscita per i seguenti protocolli: IP, ICMP, UDP e TCP.

Suggerimenti
Dal momento che per filtrare un pacchetto vengono applicate le regole una dopo l'altra, la loro sequenza è di particolare importanza. Si prega di modificare la sequenza delle regole solo quando si è completamente sicuri del risultato che si otterrà.

Pulsanti

Pulsanti	Descrizione
Aggiungi	Consente la creazione di una nuova regola. Facendo clic su questo pulsante appare la finestra di dialogo "**Aggiungi nuova regola**". In questa finestra di dialogo è possibile selezionare nuove regole.
Cancella	Elimina una regola selezionata.
In basso	Spostare una regola selezionata in una posizione verso il basso riducendo in tal modo la priorità di questa regola.
In alto	Spostare una regola selezionata in una posizione verso l'alto aumentando in tal modo la priorità di questa regola.
Rinomina	Rinomina una regola selezionata.

Suggerimenti
È possibile aggiungere nuove regole per i singoli adattatori o anche per tutti gli adattatori disponibili del computer. Per aggiungere una regola adattatore per tutti gli adattatori selezionare **Computer** nella struttura del computer visualizzata e fare clic sul pulsante **Aggiungi**.

Suggerimenti
Per modificare la posizione di una regola, è possibile anche trascinare la regola nella posizione desiderata utilizzando il mouse.

13.4.2 Regole di applicazione

Regole specifiche dell'applicazione per l'utente

Questo elenco contiene tutti gli utenti nel sistema. Qualora ci si registri come Amministratore è possibile selezionare un utente per il quale creare delle regole. Nel caso in cui non si sia in possesso di diritti privilegiati, l'elenco mostrerà esclusivamente l'utente attualmente registrato.

Elenco delle applicazioni

Questa tabella mostra l'elenco delle applicazioni per le quali è stata definita una regola. L'elenco mostra le impostazioni di ogni applicazione che è stata eseguita dall'installazione del FireWall di Avira e per la quale è stata memorizzata una regola.

Visualizzazione standard

	Descrizione
Applicazione	Nome dell'applicazione.
Modalità	Visualizza la modalità impostata della regola di applicazione : In modalità **filtrata** le regole adattatore vengono verificate ed eseguite dopo l'esecuzione della regola di applicazione. In modalità *privilegiata* le regole adattatore vengono ignorate. Facendo clic con il mouse sul link è possibile passare a un'altra modalità.
Azione	Visualizza l'azione che il FireWall Avira deve eseguire automaticamente nel caso in cui l'applicazione utilizzi la rete, indipendentemente dall'uso che ne fa. Facendo clic con il mouse sul link si ha la possibilità di passare a un altro tipo di azione. Sono disponibili i tipi di azione **Chiedi**, **Consenti** o **Rifiuta**. L'impostazione standard è **Chiedi**.

Configurazione estesa

Se si desidera regolare individualmente gli accessi alla rete di un'applicazione, è possibile creare, analogamente alle regole adattatore, specifiche regole di applicazione che si basano sui filtri di pacchetto. Per passare alla configurazione estesa delle regole di applicazione, attivare dapprima la modalità esperto. Modificare nella rubrica Firewall:: Impostazioni l'impostazione per le regole di applicazione: Attivare l'opzione **Impostazioni avanzate** e salvare l'impostazione con **Applica** oppure **OK**. Passare nella configurazione del Firewall alla rubrica **Firewall::Regole di applicazione**: nell'elenco delle regole di applicazione sarà visualizzata un'altra colonna *Filtro* con la voce *Semplice*. A questo punto è disponibile l'opzione aggiuntiva **Filtro:** *Avanzato - Azione: Regole*, che consente di passare alla configurazione estesa.

	Descrizione
Applicazione	Nome dell'applicazione.
Modalità	Visualizza la modalità impostata della regola di applicazione : In modalità **filtrata** le regole adattatore vengono verificate ed eseguite dopo l'esecuzione della regola di applicazione. In modalità *privilegiata* le regole adattatore vengono ignorate. Facendo clic con il mouse sul link è possibile passare a un'altra modalità.

Azione	Visualizza l'azione che il FireWall Avira deve eseguire automaticamente nel caso in cui l'applicazione utilizzi la rete, indipendentemente dall'uso che ne fa. Impostando *Filtro - Semplice* è possibile passare a un'altra modalità di azione facendo clic con il mouse sul collegamento. Sono disponibili i tipi di azione **Chiedi**, **Consenti, Rifiuta** o *Avanzato*. Impostando *Filtro - Avanzato* si visualizzerà la modalità di azione *regole*. Il link **Regole** apre la finestra **Regole di applicazione**, in cui è possibile salvare regole specifiche per l'applicazione.
Filtro	Permette di visualizzare la modalità di filtro. Facendo clic con il mouse sul link si ha la possibilità di passare a un altro tipo di filtro. *Semplice*: Impostando il filtro semplice l'azione indicata sarà eseguita per tutte le attività di rete dell'applicazione software. *Avanzato*: Il filtro prevede l'esecuzione delle regole salvate nella configurazione estesa.

Se si desidera impostare le regole di applicazione specificate per una applicazione, sarà sufficiente passare alla voce *Filtro* all'impostazione **Avanzato**. Nella colonna **Azione** comparirà quindi la voce *Regole*. Fare clic su **Regole** per accedere nella finestra all'impostazione di regole di applicazione specifiche.

Regole di applicazione specifiche della configurazione estesa

Utilizzando regole di applicazione specifiche è possibile consentire o rifiutare il traffico di dati specifico dell'applicazione, nonché consentire o rifiutare l'attesa passiva dalle singole porte. Sono disponibili le seguenti opzioni:

– Consenti o rifiuta l'inserimento di codice

L'inserimento di codice è una tecnica che esegue codice nello spazio indirizzi di un altro processo e obbliga tale processo a caricare una Dynamic Link Library (DLL). Questa tecnica viene utilizzata ad esempio dal malware per eseguire codice sotto la copertura di altri programmi. In questo modo è possibile, ad esempio, nascondere gli accessi Internet al FireWall. In generale l'inserimento di codice è consentito a tutte le applicazioni dotate di firma.

– Consenti o rifiuta l'attesa passiva dell'applicazione dalle porte
– Consenti o rifiuta il traffico di dati:

Consenti o rifiuta pacchetti IP in ingresso e/o in uscita

Consenti o rifiuta pacchetti TCP in ingresso e/o in uscita

Consenti o rifiuta pacchetti UDP in ingresso e/o in uscita

Per ciascuna applicazione è possibile creare un numero a piacere di regole di applicazione. Le regole di applicazione vengono eseguite nell'ordine visualizzato .

Suggerimenti
Nel caso in cui venga modificato il filtro *Esteso* di una regola di applicazione, le regole di applicazione già impostate nella configurazione estesa non vengono definitivamente eliminate, ma solo disattivate. Se si passa di nuovo al filtro *Esteso*, le regole di applicazione già impostate vengono di nuovo attivate e visualizzate nella finestra della configurazione estesa delle regole di applicazione.

Dettagli applicazione

In questa categoria vengono visualizzate informazioni dettagliate relative all'applicazione selezionata nell'elenco delle applicazioni.

	Descrizione
Nome	Nome dell'applicazione.
Percorso	Percorso completo del file eseguibile.

Pulsanti

Pulsanti	**Descrizione**
Aggiungi applicazione	Consente la creazione di una nuova regola di applicazione. Facendo clic su questo pulsante appare una finestra di dialogo. Ora è possibile selezionare un'applicazione per la quale si desidera creare una regola.
Rimuovi regola	Elimina la regola applicazione selezionata.
Carica nuovamente	Carica nuovamente la lista delle applicazioni e rifiuta al contempo tutte le modifiche apportate alle regole applicazione.

13.4.3 Fornitori affidabili

In *Fornitori affidabili* viene visualizzato un elenco dei produttori di software affidabili. È possibile rimuovere o aggiungere produttori dall'elenco utilizzando l'opzione *Fidati sempre di questo fornitore* nella finestra di pop up *Evento di rete*. È possibile consentire di default l'accesso alla rete delle applicazioni, dotate della firma dei fornitori contenuti nell'elenco, attivando l'opzione **Consenti automaticamente le applicazioni create da fornitori affidabili**.

Fornitori affidabili per l'utente

Questo elenco contiene tutti gli utenti del sistema. Qualora ci si registri come Amministratore è possibile selezionare un utente il cui elenco di fornitori affidabili si desidera esaminare o gestire. Qualora l'utente non fosse in possesso di diritti privilegiati, l'elenco mostra solamente l'utente attualmente registrato.

Consenti automaticamente applicazioni create da fornitori affidabili

Se l'opzione è attivata, viene consentito automaticamente l'accesso alla rete alle applicazioni dotate della firma dei fornitori conosciuti e affidabili. L'opzione è attivata di default.

Fornitori

L'elenco mostra tutti i fornitori classificati come affidabili.

Pulsanti

Pulsanti	Descrizione
Cancella	La voce contrassegnata viene rimossa dall'elenco dei fornitori affidabili. Per rimuovere definitivamente dall'elenco il fornitore selezionato, fare clic su **Applica** oppure**OK** nella finestra di configurazione.
Carica nuovamente	Le modifiche effettuate vengono annullate: l'ultimo elenco memorizzato viene caricato.

Suggerimenti
Se si rimuovono fornitori dall'elenco e si fa clic sul pulsante **Applica**, i fornitori vengono definitivamente eliminati dall'elenco. Non è possibile annullare la modifica con *Carica nuovamente*. È tuttavia possibile aggiungere nuovamente un fornitore all'elenco dei fornitori affidabili tramite l'opzione *Fidati sempre di questo fornitore* nella finestra di pop up *Evento di rete*.

Suggerimenti
Il FireWall dà la priorità alle regole di applicazione rispetto alle voci dell'elenco dei fornitori affidabili: se è stata creata una regole di applicazione e il fornitore dell'applicazione è compreso nell'elenco dei fornitori affidabili, la regola viene eseguita.

13.4.4 Impostazione

Impostazioni aggiuntive

Attiva firewall

Se l'opzione è attivata, il FireWall di Avira è attivo e protegge il computer dai pericoli di Internet e di altre reti.

Disattiva Windows Firewall all'avvio

Se l'opzione è attivata, Windows Firewall risulta disattivato all'avvio del computer. Questa opzione è attivata di default.

Il file host di Windows NON È BLOCCATO /È BLOCCATO

Se questa opzione è settata su BLOCCATO, il file host di Windows è protetto dalla scrittura. Non è più possibile manipolare il file. Il malware non è più, ad esempio, in grado di deviare l'utente su pagine Internet indesiderate. Di default questa opzione è impostata su NON BLOCCATO.

Timeout della regola

Blocca sempre

Se l'opzione è attivata viene mantenuta una regola che viene creata automaticamente ad esempio durante un Port-Scan.

Rimuovi regola dopo n secondi

Se l'opzione è attivata viene eliminata una regola creata, per esempio, durante un Port-Scan dopo un intervallo definito dall'utente. Questa opzione è attivata di default.

Notifiche

In Notifiche è possibile determinare al verificarsi di quali eventi si desidera ricevere un messaggio del FireWall sul desktop.

Port scan

Se l'opzione è attivata, si riceve un messaggio sul desktop quando il FireWall ha rilevato un Port-Scan.

Flooding

Se l'opzione è attivata, si riceve un messaggio sul desktop quando il FireWall ha rilevato un attacco flood.

Applicazioni bloccate

Se l'opzione è attivata, si riceve un messaggio sul desktop quando il FireWall ha rifiutato o bloccato un'attività di rete di un'applicazione.

IP bloccato

Se l'opzione è attivata, si riceve un messaggio sul desktop quando il FireWall ha rifiutato il traffico di dati da un indirizzo IP.

Regole di applicazione

Le opzioni dell'area Regole applicazione consentono di impostare le possibilità di configurazione delle regole di applicazione nella rubrica FireWall::Regole applicazione.

Impostazioni aggiuntive

Se l'opzione è attivata, è possibile regolare individualmente i diversi accessi alla rete di un'applicazione.

Impostazioni di base

Se l'opzione è attivata, è possibile impostare una sola azione per i diversi accessi alla rete dell'applicazione.

13.4.5 Impostazioni pop up

Impostazioni pop up

Verificare lo Startblock del processo

Se l'opzione è attivata, viene verificato accuratamente il batch del processo. Il FireWall parte dal presupposto che ogni processo in batch, mediante il quale il processo figlio interviene sulla rete, non sia affidabile. Pertanto in questo caso viene aperta una finestra pop up per ogni processo in batch non affidabile. Questa opzione è disattivata di default.

Mostra più finestre di dialogo per processo

Se l'opzione è attivata, viene aperta una finestra pop up ogni volta che un'applicazione tenta di creare una connessione a Internet. In alternativa, l'informazione viene presentata solo al primo tentativo di connessione. Questa opzione è disattivata di default.

Sopprimi automaticamente il messaggio pop up in modalità di riproduzione.

Se l'opzione è attivata, il FireWall di Avira passa automaticamente alla modalità di riproduzione quando sul computer viene eseguita un'applicazione in modalità a schermo intero. In modalità di riproduzione vengono utilizzate tutte le regole adattatore e di applicazione definite. Per le applicazioni per le quali non sono state definite regole con le azioni "*Consenti*" o"*Rifiuta*" l'accesso alla rete viene consentito temporaneamente, in modo che non vengano aperte finestre pop up che richiedono l'evento di rete.

Memorizza azione per questa applicazione

Sempre attivo

Se l'opzione è attivata, l'opzione "**Memorizza azione per questa applicazione**" della finestra di dialogo "**Evento di rete**" è attivata di default. Questa opzione è attivata di default.

Sempre disattivato

Se l'opzione è attivata, l'opzione "**Memorizza azione per questa applicazione**" della finestra di dialogo "**Evento di rete**" è disattivata di default.

Consenti applicazione con firma

Se l'opzione è attivata, l'opzione "**Memorizza azione per questa applicazione**" della finestra di dialogo "**Evento di rete**" è attivata di default per l'accesso alla rete di applicazioni firmate di produttori specifici. Tali produttori sono: Microsoft, Mozilla, Opera, Yahoo, Google, Hewlet Packard, Sun,Skype, Adobe, Lexmark, Creative Labs, ATI, nVidia.

Ricorda stato più recente

Se l'opzione è attivata, l'opzione "**Memorizza azione per questa applicazione**" della finestra di dialogo "**Evento di rete**" viene gestita come per l'ultimo evento di rete. Se nell'ultimo evento di rete l'opzione "**Memorizza azione per questa applicazione**" era attivata, risulta attiva anche per gli eventi di rete successivi. Se nell'ultimo evento di rete l'opzione "**Memorizza azione per questa applicazione"** era disattivata, risulta disattivata anche per gli eventi di rete successivi.

Visualizza dettagli

In questo gruppo di opzioni di configurazione è possibile definire la visualizzazione di informazioni dettagliate nella finestra **Evento di rete**.

Visualizza dettagli su richiesta

Se l'opzione è attivata, le informazioni dettagliate nella finestra "*Evento di rete*" vengono visualizzate solo su richiesta, ovvero facendo clic sul pulsante "**Visualizza dettagli"** nella finestra "*Evento di rete*".

Visualizza sempre dettagli

Se l'opzione è attivata, le informazioni dettagliate nella finestra "*Evento di rete*" vengono sempre visualizzate.

Ricorda stato più recente

Se l'opzione è attivata, la visualizzazione delle informazioni dettagliate viene gestita come per l'evento di rete precedente. Se per l'ultimo evento di rete le informazioni dettagliate erano visualizzate o richiamate, anche negli eventi successivi vengono visualizzate. Se per l'ultimo evento di rete le informazioni dettagliate non erano visualizzate o richiamate, anche negli eventi successivi non vengono visualizzate.

Consenti privilegiati

In questo gruppo di opzioni di configurazione è possibile impostare lo stato dell'opzione *Consenti privilegiati* nella finestra **Evento di rete**.

Sempre attivo

Se l'opzione è attivata, l'opzione "*Consenti privilegiati*" nella finestra "*Evento di rete*" è attivata di default.

Sempre disattivato

Se l'opzione è attivata, l'opzione "*Consenti privilegiati*" nella finestra "*Evento di rete*" è disattivata di default.

Ricorda stato più recente

Se l'opzione è attivata, lo stato dell'opzione "*Consenti privilegiati*" nella finestra "*Evento di rete*" viene gestito come per l'evento di rete precedente: Se durante l'esecuzione dell'ultimo evento di rete, l'opzione "*Consenti privilegiati*" è attivata, l'opzione risulta attivata di default anche durante l'evento di rete successivo. Se durante l'esecuzione dell'ultimo evento di rete l'opzione "*Consenti privilegiati*" era disattivata, l'opzione risulta disattivata di default anche durante l'evento di rete successivo.

13.5 WebGuard

La rubrica WebGuard della configurazione è dedicata alla configurazione di WebGuard.

13.5.1 Cerca

WebGuard consente di proteggersi da virus e malware, che giungono sul computer attraverso i siti Web caricati da Internet nel browser Web. Nella rubrica *Scansione* è possibile impostare il comportamento di WebGuard.

Cerca

Attiva WebGuard

Se l'opzione è attivata, i siti web, richiesti tramite un browser Internet, vengono controllati per verificare la presenza di virus e malware: WebGuard monitora i file trasmessi da Internet tramite il protocollo HTTP alle porte 80, 8080 e 3128. In caso di rilevamento di siti Web infetti, il caricamento del sito Web viene bloccato. Se l'opzione è disattivata, il servizio di WebGuard rimane attivo, tuttavia la scansione per verificare la presenza di virus e malware resta disattivata.

Suggerimenti
Per utilizzare la funzione di protezione per bambini, è necessario attivare WebGuard.

Protezione drive-by

La protezione drive-by consente di effettuare impostazioni per bloccare gli iframe, detti anche inline frame. Gli iframe sono elementi HTML, ovvero elementi di siti Internet, che delimitano un'area di un sito Web. Gli iframe consentono di caricare e visualizzare altri contenuti Web, per lo più di altri URL, come documenti indipendenti in una sottofinestra del browser. Gli iframe vengono principalmente utilizzati per i banner pubblicitari. In alcuni casi gli iframe vengono utilizzati per nascondere virus e malware. In questi casi l'area dell'iframe nel browser è appena o per niente visibile. L'opzione *Blocca iframe sospetti* consente di controllare e di bloccare il caricamento di iframe.

Blocca I-Frames sospetti

Se l'opzione è attivata, gli iframe dei siti richiesti vengono verificati in base a determinati criteri. Se in uno dei siti Web richiesti sono presenti iframe sospetti, l'iframe viene bloccato. Nella finestra dell'iframe viene visualizzato un messaggio di errore.

Standard

Se l'opzione è attivata, gli iframe con contenuti sospetti vengono bloccati.

Avanzato

Se l'opzione è attivata, gli iframe con contenuti sospetti e gli iframe, utilizzati in un modo sospetto, vengono bloccati. Un utilizzo sospetto degli iframe può verificarsi quando l'iframe è di dimensioni molto piccole e quindi è appena o per niente visibile nel browser oppure quanto l'iframe è stato collocato in una posizione insolita del sito web.

13.5.1.1. Azione per i rilevamenti

Azione per i rilevamenti

È possibile stabilire delle azioni che WebGuard deve eseguire quando viene rilevato un virus o un programma indesiderato.

Interattivo

Se l'opzione è attivata, durante la scansione diretta in caso di rilevamento di un virus o di un programma indesiderato, viene visualizzata una finestra di dialogo nella quale è possibile scegliere come procedere con i file infetti. Questa opzione è attivata di default.

É possibile reperire maggiori informazioni qui.

Visualizza barra di progressione

Se l'opzione è attivata, quando un download o lo scaricamento del contenuto di pagine Web supera un timeout di 20 secondi viene visualizzato un messaggio sul desktop con una barra di progressione per il download. Questo messaggio sul desktop è utile in particolare per il controllo del download da pagine Web con grandi volumi di dati: navigando con WebGuard i contenuti delle pagine Web non vengono caricati gradualmente nel browser Internet poiché, prima di essere visualizzati nel browser Internet vengono scansionati alla ricerca di virus e malware. Questa opzione è disattivata di default.

Automatico

Se l'opzione è attivata, in caso di rilevamento di un virus o di programmi indesiderati non appare alcuna finestra di dialogo in cui selezionare l'azione da eseguire. WebGuard reagisce conformemente alle impostazioni definite precedentemente dall'utente in questa sezione.

Azione primaria

L'azione primaria è l'azione che viene eseguita quando WebGuard rileva un virus o un programma indesiderato.

Nega accesso

Il sito Web richiesto dal server Web o i dati e i file trasferiti non vengono inviati al proprio browser Web. Nel browser Web viene visualizzato un messaggio di errore relativo al divieto di accesso. WebGuard inserisce il rilevamento nel file di report, a condizione che la funzione di report sia attivata.

isola

Il sito Web richiesto dal server Web o i dati e i file trasferiti vengono inviati in quarantena in caso di rilevamento di un virus o di un malware. Il file infetto può essere ripristinato dal Gestore della quarantena se ha un valore informativo, oppure, se necessario, inviato ad Avira Malware Research Center.

ignora

Il sito Web richiesto dal server Web o i dati e i file trasferiti vengono inoltrati da WebGuard al proprio browser Web. L'accesso al file viene consentito e il file viene mantenuto.

Attenzione
Il file infetto rimane attivo sul computer! Questo potrebbe causare danni notevoli al computer!

13.5.1.2. Accessi bloccati

In **Accessi bloccati** è possibile immettere i tipi di file e i tipi di MIME (tipi di contenuto dei dati trasmessi) che devono essere bloccati da WebGuard. Il filtro Web consente di bloccare URL noti indesiderati, quali gli URL di phishing e malware. WebGuard impedisce il trasferimento dei file da Internet al computer.

Tipi di file / tipi di MIME che devono essere bloccati da WebGuard (definiti dall'utente)

Tutti i tipi di file e i tipi di MIME (tipo di contenuto dei dati trasmessi) nell'elenco vengono bloccati da WebGuard.

Campo

In questo campo immettere i nomi dei tipi di MIME e dei tipi di file che devono essere bloccati da WebGuard. Per i tipi di file, inserire l'estensione del file, ad esempio **.htm**. Per i MIME segnalare il tipo di supporto ed eventualmente il sottotipo. I due dati vengono separati da una semplice barra, ad esempio **video/mpeg** o **audio/x-wav**.

Suggerimenti
I file che sono già stati salvati sul computer come file Internet temporanei, vengono bloccati da WebGuard, ma possono comunque venire caricati dal computer localmente dal browser Internet. I file temporanei Internet sono file che vengono memorizzati sul computer dal browser Internet per poter visualizzare le pagine Web più rapidamente.

Suggerimenti
Nell'elenco dei tipi di file e di MIME da bloccare vengono ignorate le voci dell'elenco dei tipi di file e di MIME da tralasciare in WebGuard::Scansione::Eccezioni.

Suggerimenti
Nell'immissione dei tipi di file e di MIME non è possibile utilizzare wildcard (wildcard * per un numero a piacere di caratteri o ? per un solo carattere).

Tipi di MIME: esempi per tipi di supporto:

– `text` = per file di testo
– `image` = per file di grafica
– `video` = per file video
– `audio` = per file audio
– `application` = per file associati a un programma specifico

Esempi: tipi di file e di MIME da escludere

– `application/octet-stream` = i file del tipo MIME application/octet-stream (eseguibili *.bin, *.exe, *.com, *dll, *.class) vengono bloccati da WebGuard.
– `application/olescript` = i file del tipo MIME application/olescript (file di script ActiveX *.axs) vengono bloccati da WebGuard.
– `.exe` = tutti i file con l'estensione .exe (file eseguibili) vengono bloccati da WebGuard.
– `.msi` = tutti i file con estensione .msi (file di Windows Installer) vengono bloccati da WebGuard.

Aggiungi

Con il pulsante è possibile accettare i MIME e il tipo di file indicati nella finestra.

Elimina

Il pulsante elimina una voce selezionata nella lista. Questo pulsante non è attivo se non è selezionata alcuna voce.

Filtro Web

Il filtro Web dispone di una banca dati interna aggiornata quotidianamente nella quale gli URL sono classificati in base a criteri di contenuto.

Attiva filtro Web

Se l'opzione è attivata, vengono bloccati tutti gli URL appartenenti alle categorie selezionate nell'elenco del filtro Web.

Elenco filtro Web

Nell'elenco del filtro Web è possibile selezionare le categorie di contenuto i cui URL devono essere bloccati da WebGuard.

Suggerimenti
Il filtro Web viene ignorato per le voci dell'elenco degli URL da tralasciare in WebGuard::Scansione::Eccezioni.

Suggerimenti
Vengono categorizzati come URL di spam gli URL diffusi con i messaggi email di spam. La categoria Frode e inganno comprende i siti web con 'abbonamenti-trappola' e altre offerte di servizi i cui costi vengono occultati dal fornitore.

13.5.1.3. Eccezioni

Queste opzioni consentono di escludere tipi di MIME (tipi di contenuto dei file trasferiti) e tipi di file per gli URL (indirizzi Internet) dalla scansione di WebGuard. Gli URL e i tipi di MIME indicati vengono ignorati da WebGuard, ovvero durante la trasmissione al computer dell'utente non viene effettuata la scansione di questi dati per verificare la presenza di virus e malware.

Tipi di MIME da omettere dal WebGuard

In questo campo è possibile selezionare tipi di MIME (tipi di contenuto dei dati trasferiti) che devono essere esclusi dalla scansione di WebGuard.

Tipi di file / tipi di MIME da escludere da WebGuard (definiti dall'utente)

Tutti i tipi di file e i tipi di MIME (tipi di contenuto dei dati trasferiti) nell'elenco vengono esclusi dalla scansione di WebGuard.

Campo

Inserire in questo campo i nomi dei tipi di MIME e di file che si intendono escludere dalla scansione di WebGuard. Per i tipi di file, inserire l'estensione del file, ad esempio **.htm**. Per i MIME segnalare il tipo di supporto ed eventualmente il sottotipo. I due dati vengono separati da una semplice barra, ad esempio **video/mpeg** o **audio/x-wav**.

Suggerimenti
Nell'immissione dei tipi di file e di MIME non è possibile utilizzare wildcard (wildcard * per un numero a piacere di caratteri o ? per un solo carattere).

Attenzione
Tutti i tipi di file e di contenuto dell'elenco delle eccezioni vengono caricati nel browser Internet senza ulteriori verifiche di blocco dell'accesso (elenco dei tipi di file e di MIME da bloccare in WebGuard::Scansione::Accessi bloccati) o di WebGuard: Per tutte le voci dell'elenco delle eccezioni viene ignorato il contenuto dell'elenco dei tipi di file e di MIME da bloccare. Non viene eseguita alcuna scansione per virus e malware.

Tipi MIME: esempio per tipi di supporto:

- `text` = per file di testo
- `image` = per file di grafica
- `video` = per file video
- `audio` = per file audio
- `application` = per file associati a un programma specifico

Esempi: tipi di file e di MIME da tralasciare

- `audio/` = tutti i file del tipo di supporto audio vengono esclusi dalla scansione di WebGuard
- `video/quicktime` = tutti i file video del sottotipo Quicktime (*.qt, *.mov) vengono esclusi dalla scansione di WebGuard
- `.pdf` = tutti i file Adobe-PDF vengono esclusi dalla scansione di WebGuard.

Aggiungi

Con il pulsante è possibile accettare i MIME e il tipo di file indicati nella finestra.

Elimina

Il pulsante elimina una voce selezionata nella lista. Questo pulsante non è attivo se non è selezionata alcuna voce.

URL da omettere per WebGuard

Tutti gli URL di questo elenco vengono esclusi dalla scansione di WebGuard.

Campo

Immettere in questo campo gli URL (indirizzi Internet) che devono essere esclusi dalla scansione di WebGuard, ad esempio **www.domainname.com**. È possibile inserire parti di URL definendo il livello del dominio con punti iniziali o finali: .domainname.it per tutte le pagine e i tutti i domini secondari del dominio. Per indicare una pagina Web con un dominio di livello superiore a piacere (.com o .net), utilizzare un punto finale: **domainname.**. Se si utilizza una sequenza di caratteri senza punto iniziale o finale, viene interpretata come dominio di livello superiore, ad es. **net** per tutti i domini NET (www.domain.net).

Suggerimenti
Nell'immissione degli URL è possibile utilizzare anche wildcard * per un numero di caratteri a piacere. Per definire il livello del dominio, utilizzare anche punti iniziali o finali in combinazione con wildcard:
.domainname.*
*.domainname.com
.*name*.com (valido ma non consigliato)
I dati senza punti quali *name* vengono interpretati come parti di dominio di livello superiore e non sono consigliati.

Attenzione
Tutti i siti Web nell'elenco degli URL da tralasciare vengono caricati nel browser Internet senza ulteriore controllo del filtro Web o di WebGuard: per tutte le voci dell'elenco degli URL da tralasciare vengono ignorate le voci del filtro Web (vedere WebGuard::Scansione::Accessi bloccati). Non viene eseguita alcuna scansione per virus e malware. Si consiglia pertanto di escludere dalla scansione di WebGuard solo URL affidabili.

Aggiungi

Con il pulsante è possibile accettare nella finestra gli URL (indirizzi Internet) indicati.

Elimina

Il pulsante elimina una voce selezionata nella lista. Questo pulsante non è attivo se non è selezionata alcuna voce.

Esempi: URL da tralasciare

– `www.avira.com` -OPPURE- `www.avira.com/*`

= Tutti gli URL con dominio 'www.avira.com' vengono esclusi dalla scansione di WebGuard: www.avira.com/en/pages/index.php, www.avira.com/en/support/index.html, www.avira.com/en/download/index.html,.. Gli URL con dominio www.avira.com/it vengono esclusi dalla scansione di WebGuard.

– `avira.com` -OPPURE- `*.avira.com`

= Tutti gli URL con dominio di livello secondario o superiore 'avira.com' vengono esclusi dalla scansione di WebGuard. Tali dati comprendono tutti i domini secondari esistenti di '.avira.com': www.avira.com, forum.avira.com,...

– `avira.` -OPPURE- `*.avira.*`

= Tutti gli URL con dominio di livello secondario 'avira' vengono esclusi dalla scansione di WebGuard. Tali dati comprendono tutti i domini esistenti di livello superiore o i domini secondari di '.avira.': www.avira.com, www.avira.com/it, forum.avira.com,...

– `.*domain*.*`

Tutti gli URL che contengono un dominio di livello secondario con la sequenza di caratteri 'domain', vengono esclusi dalla scansione di WebGuard: www.domain.com, www.new-domain.it, www.sample-domain1.it, ...

– `net` -OPPURE- `*.net`

=Tutti gli URL con dominio di livello superiore 'net' vengono esclusi dalla scansione di WebGuard: www.name1.net, www.name2.net,...

Attenzione
Indicare tutti gli URL che si desidera escludere dalla scansione di WebGuard nel modo più preciso possibile. Evitare l'immissione di tutti i domini di livello superiore o parti di nomi di domini secondari, poiché vi è il rischio che le pagine Internet, che diffondono malware e programmi indesiderati mediante dati globali, vengano escluse dalla scansione di WebGuard come eccezione. Si consiglia di immettere almeno il dominio secondario e il dominio di livello superiore completi: domainname.com

13.5.1.4. Euristico

Questa rubrica di configurazione contiene le impostazioni per l'euristica del motore di ricerca.

I prodotti AntiVir contengono un'euristica molto efficace, che consente di riconoscere in modo proattivo malware sconosciuti, ovvero prima che venga creata una firma speciale dei virus contro il parassita e che venga inviato un aggiornamento della protezione antivirus. Il riconoscimento dei virus avviene attraverso un'approfondita analisi e indagine del relativo codice in base alle funzioni tipiche dei malware. Se il codice esaminato corrisponde a tali caratteristiche tipiche viene segnalato come sospetto. Ciò non significa necessariamente che il codice indichi effettivamente la presenza di un malware; potrebbe trattarsi anche di messaggi di errore. La decisione su come procedere con il codice spetta all'utente stesso, ad esempio sulla base delle sue conoscenze relativamente all'attendibilità della fonte che contiene il codice segnalato.

Macrovirus euristico

Macrovirus euristico

Il prodotto AntiVir acquistato contiene un macrovirus euristico molto efficace. Se l'opzione è attivata, in caso di riparazione possibile tutte le macro del documento infetto vengono eliminate, in alternativa i documenti sospetti vengono solo segnalati, l'utente riceverà quindi un avviso. Questa impostazione è attivata di default e viene consigliata.

Advanced Heuristic Analysis and Detection (AHeAD)

Attiva AHeAD

Il programma AntiVir contiene, grazie alla tecnologia AntiVir AHeAD, un'euristica molto efficace, in grado di riconoscere anche malware sconosciuti (nuovi). Se l'opzione è attivata, è possibile impostare il grado di rigidità dell'euristica. Questa opzione è attivata di default.

Livello di rilevamento basso

Se l'opzione è attivata, viene riconosciuto un numero inferiore di malware sconosciuti e il rischio di possibili rilevamenti di errore è limitato.

Livello di rilevamento medio

Questa impostazione è attivata di default, se è stata scelta l'applicazione di questa euristica.

Livello di riconoscimento elevato

Se l'opzione è attivata, viene riconosciuto un numero significativamente maggiore di malware sconosciuti, ma possono verificarsi messaggi di errore.

13.5.2 Report

WebGuard possiede una funzione di log molto vasta che può fornire all'utente o all'amministratore informazioni esatte sulla modalità di un rilevamento.

Funzione di log

In questo gruppo viene definita la portata contenutistica del file di report.

Disabilitato

Se l'opzione è attivata, WebGuard non crea alcun protocollo.
In casi eccezionali si può rinunciare alla funzione di report, solo se si eseguono test con molti virus o programmi indesiderati.

Standard

Se l'opzione è attivata, WebGuard registra informazioni importanti (su rilevamenti, avvisi ed errori) nel file di report, mentre le informazioni meno importanti vengono ignorate per maggiore chiarezza. Questa opzione è attivata di default.

Avanzato

Se l'opzione è attivata, WebGuard registra nel file di report anche le informazioni meno importanti.

Completo

Se l'opzione è attivata, WebGuard registra tutte le informazioni - anche quelle relative alla dimensione del file, al tipo, alla data, ecc. - nel file di report.

Limitazioni del file di report

Limita la dimensione a n MB

Se l'opzione è attivata, il file di report può essere limitato a una determinata dimensione; valori possibili: da 1 a 100 MB. Con la limitazione del file di report si introduce un intervallo di circa 50 kilobyte per non sovraccaricare il processore. Se la dimensione del file di report supera la dimensione fissata di 50 Kilobyte, vengono automaticamente eliminate le voci più vecchie fin quando non si raggiunge una dimensione inferiore del 20% .

Backup file report prima della limitazione

Se l'opzione è attivata il file del report viene salvato prima dell'abbreviazione.

Scrivi la configurazione nel file di report

Se l'opzione è attivata, la configurazione utilizzata della scansione in tempo reale viene riportata nel file di report.

Suggerimenti
Se non sono state specificate limitazioni per i file di report, vengono automaticamente eliminate le voci più vecchie quando il file di report raggiunge le dimensioni di 100 MB. Viene eliminato un numero di voci tali da consentire al file di report di raggiungere una dimensione di 80 MB.

13.6 Protezione bambini

13.6.1 Parental control

Il programma AntiVir è provvisto di una funzione di protezione bambini per filtrare offerte Internet indesiderate o illegali e per la limitazione temporale dell'utilizzo di Internet. La funzione di protezione bambini fa parte del componente WebGuard. È possibile assegnare ruoli utente agli utenti del computer. I ruoli utente sono configurabili e comprendono un set di regole con i seguenti criteri:

- URL consentiti o non consentiti (indirizzi Internet)
- Categorie di contenuti non consentite
- Durata dell'utilizzo di Internet ed eventuali intervalli di tempo consentiti per l'utilizzo nei giorni della settimana

Per bloccare i contenuti Internet in base a determinate categorie vengono utilizzati elenchi di filtri URL efficaci, nei quali gli URL vengono categorizzati in gruppi di contenuti in base ai contenuti delle pagine Internet. Gli elenchi dei filtri URL vengono aggiornati, adattati e ampliati più volte ogni ora. I ruoli bambino, adolescente, adulto sono preconfigurati con le categorie non consentite corrispondenti.

L'utilizzo temporale di Internet viene stabilito sulla base di richieste di collegamento a Internet che avvengono con un intervallo minimo di 5 minuti.

Se la protezione bambini è attivata, durante la navigazione in Internet tutti i siti Web richiesti nel browser vengono verificati in base al ruolo utente. In caso di siti Web non consentiti, il sito Web viene bloccato e viene visualizzato un messaggio nel browser. In caso di superamento della durata di utilizzo consentita oppure se l'utilizzo supera l'intervallo consentito, le pagine Web richiamate vengono bloccate. Nel browser viene visualizzato un messaggio.

Attenzione
Si osservi che è necessario attivare il servizio WebGuard per poter utilizzare la funzione protezione bambini.

Attenzione
Quando si attiva la protezione bambini, proteggere la configurazione del programma AntiVir mediante una password. Se la configurazione non è protetta tramite password, tutti gli utenti del computer potranno modificare o disattivare le impostazioni della protezione bambini. È possibile attivare la password in Generale::Password.

Se è stata assegnata una password per la protezione bambini, la configurazione per la protezione bambini viene nascosta e viene visualizzato il pulsante *Protetto da password*.

Protetto da password

Premere il pulsante "**Protetto da password"** e inserire la password per la protezione bambini nella finestra "*Inserimento password"* per abilitare la configurazione della protezione bambini.

Attiva protezione bambini

Se l'opzione è attivata, tutti i siti web, richiesti durante la navigazione in Internet, vengono verificati in base al ruolo assegnato all'utente registrato nella protezione per bambini. I siti web richiesti vengono bloccati se sono stati classificati come non consentiti nell'ambito del ruolo assegnato.

Suggerimenti
Se la protezione bambini è attivata, l'utente del computer al quale non è stato assegnato alcun ruolo nella configurazione della protezione bambini viene classificato di default dal programma come *Standard* con il ruolo *Bambino*. È possibile modificare il ruolo dell'utente standard.
Dopo l'installazione vengono applicati i ruoli utente bambino, adolescente e adulto. Nei ruoli preconfigurati, la limitazione temporale dell'utilizzo di Internet è disattivata.

Selezione utente

Elenco utenti - Ruolo

Nell'elenco vengono visualizzati tutti gli utenti con il relativo ruolo assegnato. Quando si aggiunge un utente, il programma assegna di default il ruolo *Bambino*. Facendo clic con il mouse sul ruolo visualizzato, è possibile passare a un altro ruolo.

Utente

L'elenco contiene tutti gli utenti del sistema.

Aggiungi

Il pulsante consente di aggiungere l'utente selezionato all'elenco degli utenti protetti.

Elimina

Il pulsante consente di eliminare la voce dell'elenco selezionata.

Suggerimenti
Non è possibile eliminare l'utente standard.

Ruoli

Elenco

Nell'elenco vengono visualizzati tutti i ruoli immessi. Facendo doppio clic su un ruolo, si apre la finestra di dialogo per la definizione del ruolo.

Campo

Immettere nel campo il nome del ruolo che si desidera aggiungere ai ruoli utente.

Modifica

Il pulsante "*Modifica"* consente di configurare il ruolo selezionato. Viene visualizzata una finestra di dialogo nella quale è possibile definire per il ruolo URL consentiti e non consentiti e contenuti web non consentiti in base a categorie.

Aggiungi

Il pulsante consente di aggiungere all'elenco dei ruoli disponibili il ruolo immesso nel campo.

Elimina

Il pulsante consente di eliminare dall'elenco il ruolo selezionato.

Suggerimenti
Non è possibile eliminare i ruoli già assegnati a un utente.

Proprietà del ruolo

Il pulsante *Modifica* consente di passare alla finestra di dialogo *Proprietà del ruolo* nella quale è possibile definire il ruolo utente con gli URL consentiti e non consentiti e i contenuti Web non consentiti. Sono disponibili le seguenti opzioni:

- Non consentire l'accesso agli URL
- Consenti l'accesso agli URL
- Blocca i contenuti Web: è possibile selezionare categorie per i contenuti Web che devono essere bloccati.
- Limita temporalmente l'utilizzo di Internet: è possibile impostare una durata di utilizzo consentita (giornaliera, settimanale, mensile). È possibile consentire intervalli di utilizzo precisi per ogni giorno della settimana.

13.7 Backup

La rubrica Backup della configurazione è dedicata alla configurazione del componente backup di Avira.

13.7.1 Impostazione

In **Impostazioni** è possibile configurare il comportamento del componente Backup.

Impostazione

Esegui backup solo file modificati

Se l'opzione è attivata viene creato un backup incrementale: vengono memorizzati nel profilo di backup solo i file che sono stati modificati dopo l'ultimo backup. Se l'opzione è disattivata, ogni volta che si memorizza un profilo di backup viene eseguito un backup completo: tutti i file nel profilo di backup vengono memorizzati. L'opzione è normalmente attivata e consigliata poiché i backup incrementali sono più rapidi e consumano meno risorse dei backup di tutti i dati.

Verifica malware prima del backup

Se l'opzione è attivata, i file da memorizzare vengono controllati per verificare la presenza di virus e malware al momento del backup. I file infetti non vengono salvati. Questa opzione normalmente è attivata e consigliata.

13.7.2 Eccezioni

In Eccezioni è possibile definire quali oggetti file e tipi di file inserire o meno nel backup.

Oggetti file da escludere dal backup

L'elenco in questa finestra contiene file e percorsi che non devono essere memorizzati in un backup.

Suggerimenti
Le voci dell'elenco non possono superare complessivamente i 6000 caratteri.

Suggerimenti
I file inseriti in questa lista vengono segnalati nel file di report.

Campo

In questo campo è necessario immettere i nomi degli oggetti file che non si desidera memorizzare. Normalmente viene indicato il percorso di una directory temporanea per le impostazioni locali dell'utente registrato.

Il pulsante apre una finestra nella quale si ha la possibilità di selezionare il file o il percorso desiderato.
Se è stato immesso un nome file con il percorso completo, tale file non verrà memorizzato. Se è stato immesso un nome file senza percorso, tutti i file con quel nome (indipendentemente dal percorso e dal drive) non vengono memorizzati.

Aggiungi

Con il pulsante è possibile accettare il file indicato nel campo nella finestra di visualizzazione.

Elimina

Il pulsante elimina una voce selezionata nella lista. Questo pulsante non è attivo se non è selezionata alcuna voce.

Resetta lista

Questo pulsante ripristina i valori standard predefiniti.

Prestare attenzione ai seguenti punti:

– Le wildcard * (numero di caratteri desiderato) e ? (un solo carattere) sono consentite solo nei nomi del file.
– L'elenco viene elaborato dall'alto verso il basso.
– Se una directory viene esclusa, anche tutte le sottodirectory che contiene vengono escluse automaticamente.
– È possibile anche escludere singole estensioni di file (incluse le wildcard).
– Per escludere oggetti anche quando vi si accede con nomi di file DOS brevi (convenzione dei nomi di DOS 8.3), è necessario inserire nell'elenco il nome breve del file corrispondente.

Suggerimenti
Un nome di file che contiene wildcard non deve concludersi con una barra inversa.

Ad esempio:

```
C:\Programmi\Applicazione\applic*.exe\
```

Questa voce non è valida e non viene considerata come un'eccezione!

Esempi:

```
applicazione.exe
\Programmi\
```

```
C:\*.*
C:\*
*.exe
*.xl?
*.*
C:\Programmi\Applicazioni\applicazione.exe
C:\Programmi\Applicazioni\applicaz*.exe
C:\Programmi\Applicazioni\applicaz*
C:\Programmi\Applicazioni\applicaz????.e*
C:\Programmi\
C:\Programmi
C:\Programmi\Applicazioni\*.mdb
```

Liste estensioni file

Considerare tutte le estensioni dei file

Se l'opzione è attivata tutti i file nel profilo di backup vengono memorizzati.

Attiva estensioni dei file da escludere dal backup

Se l'opzione è attivata vengono salvati tutti i file nel profilo di backup, tranne quelli con estensione corrispondente alle estensioni riportate nell'elenco delle estensioni dei file da escludere.

Estensioni file

Questo pulsante consente di richiamare una finestra di dialogo in cui vengono visualizzate tutte le estensioni dei file che non vengono memorizzati in un backup attivando l'opzione "**Estensioni dei file da escludere"**. Tra le estensioni sono presenti voci standard, ma è possibile anche aggiungere o eliminare voci.

Attiva elenco delle estensioni dei file da considerare per il backup

Se l'opzione è attivata vengono memorizzati solo i file con estensione compresa nell'elenco delle estensioni dei file da considerare.

Estensioni file

Questo pulsante consente di richiamare una finestra di dialogo in cui vengono visualizzate tutte le estensioni dei file che vengono memorizzati in un backup attivando l'opzione "**Estensioni dei file da considerare**". Tra le estensioni sono presenti voci standard, ma è possibile anche aggiungere o eliminare voci.

13.7.3 Report

Il componente Backup offre una vasta funzione di log.

Funzione di log

In questo gruppo viene definita la portata contenutistica del file di report.

Disabilitato

Se l'opzione è attivata, il componente Backup non crea alcun log. Rinunciare al log solo in casi eccezionali.

Standard

Se l'opzione è attivata, il componente Backup raccoglie informazioni importanti (per la memorizzazione, per i rilevamenti dei virus, per avvisi ed errori) nel file di report, mentre le informazioni meno importanti vengono ignorate per maggiore chiarezza. Questa opzione è attivata di default.

Avanzato

Se l'opzione è attivata, il componente Backup registra nel file di report anche le informazioni meno importanti.

Completo

Se l'opzione è attivata, il componente Backup registra tutte le informazioni sul backup e sulla scansione per i virus nel file di report.

13.8 Aggiornamento

Nella rubrica *Aggiornamento* configurare l'esecuzione automatica degli aggiornamenti. È possibile impostare diversi intervalli di aggiornamento, nonché attivare o disattivare l'aggiornamento automatico.

Aggiornamento automatico

Attiva

Se l'opzione è attivata, gli aggiornamenti automatici vengono eseguiti nell'intervallo di tempo indicato, nonché al verificarsi degli eventi attivati.

Aggiornamento automatico ogni n giorni / ore / minuti

In questo campo è possibile indicare l'intervallo in cui devono essere eseguiti gli aggiornamenti automatici. Per modificare l'intervallo di aggiornamento, è possibile indicare un dato temporale nel campo e modificarlo mediante i tasti freccia a destra del campo.

Avvia il job all'avvio della connessione Internet (dial-up)

Se l'opzione è attivata, oltre all'intervallo di aggiornamento stabilito, il job di aggiornamento viene eseguito quando si attiva una connessione a Internet.

Ripeti job se il tempo è scaduto

Se l'opzione è attivata, vengono eseguiti job di aggiornamento scaduti che non è stato possibile eseguire al momento designato, ad esempio perché il computer era spento.

13.8.1 Aggiornamento di prodotto

In **Aggiornamento prodotto** configurare l'esecuzione degli aggiornamenti del prodotto o la notifica della disponibilità di tali aggiornamenti.

Aggiornamenti prodotto

Scarica aggiornamenti del prodotto e installa automaticamente

Se l'opzione è attivata, gli aggiornamenti del prodotto vengono scaricati e installati automaticamente, non appena si rendono disponibili, dai componenti di aggiornamento. Gli aggiornamenti del file di definizione dei virus e del motore di ricerca avvengono sempre e indipendentemente da questa impostazione. Le premesse per utilizzare questa opzione sono: configurazione completa dell'aggiornamento e collegamento esistente a un server di download.

Scaricare aggiornamenti del prodotto. Se è necessario riavviare, installare l'aggiornamento dopo il successivo riavvio del sistema, altrimenti eseguire immediatamente l'installazione.

Se l'opzione è attivata, gli aggiornamenti del prodotto vengono scaricati non appena disponibili. L'aggiornamento viene installato automaticamente dopo il download dei file di aggiornamento, qualora non sia necessario il riavvio. Se si tratta di un aggiornamento del prodotto che richiede il riavvio del computer, tale aggiornamento non viene eseguito subito dopo il download dei file di aggiornamento, bensì solo dopo il successivo riavvio del sistema effettuato dall'utente. Il vantaggio che ne deriva è che il riavvio non viene eseguito mentre l'utente sta lavorando al computer. Gli aggiornamenti del file di definizione dei virus e del motore di ricerca avvengono sempre e indipendentemente da questa impostazione. Le premesse per utilizzare questa opzione sono: configurazione completa dell'aggiornamento e collegamento esistente a un server di download.

Avvisa quando sono disponibili nuovi aggiornamenti del prodotto

Se l'opzione è attivata, si viene avvisati solo se sono disponibili nuovi aggiornamenti per il prodotto. Gli aggiornamenti del file di definizione dei virus e del motore di ricerca avvengono sempre e indipendentemente da questa impostazione. Le premesse per utilizzare questa opzione sono: configurazione completa dell'aggiornamento e collegamento esistente a un server di download. La notifica avviene tramite un messaggio sul desktop sotto forma di una finestra di pop up e tramite un avviso dell'Updater nel Control Center in Panoramica ::Eventi.

Avvisa nuovamente dopo n giorno(i)

Indicare in questo campo dopo quanti giorni si desidera ricevere nuovamente la notifica relativa alla disponibilità degli aggiornamenti del prodotto, qualora l'aggiornamento del prodotto non sia stato eseguito alla prima notifica.

Non scaricare aggiornamenti prodotto

Se l'opzione è attivata, non si effettuano aggiornamenti automatici o notifiche se sono disponibili aggiornamenti del prodotto mediante l'Updater. Gli aggiornamenti del file delle definizioni dei virus e del motore di ricerca avvengono sempre indipendentemente da questa impostazione.

Importante
L'aggiornamento del file di definizione dei virus e del motore di ricerca avviene contestualmente a ogni aggiornamento effettuato, indipendentemente dalle impostazioni per l'aggiornamento di prodotto (a questo proposito vedere cap. Aggiornamenti).

Suggerimenti
Se è stata attivata l'opzione per l'aggiornamento automatico del prodotto, è possibile configurare ulteriori opzioni di notifica e possibilità di interruzione del riavvio in Impostazioni riavvio.

13.8.2 Impostazioni di riavvio

Quando viene eseguito un aggiornamento del programma AntiVir, può essere necessario un riavvio del sistema. Se è stata impostata un'esecuzione automatica dell'aggiornamento del prodotto in Aggiornamento::Aggiornamento prodotto, è possibile scegliere fra diverse opzioni di notifica e per l'interruzione del riavvio in **Impostazioni riavvio**.

Suggerimenti
Nell'effettuare le impostazioni di riavvio, si noti che nella configurazione è possibile scegliere fra due opzioni per l'esecuzione degli aggiornamenti del prodotto con riavvio necessario del computer, in Aggiornamento::Aggiornamento prodotto:

Esecuzione automatica dell'aggiornamento del prodotto con riavvio del sistema necessario non appena è disponibile l'aggiornamento: l'aggiornamento e il riavvio vengono eseguiti quando l'utente sta utilizzando il computer. Se è stata attivata questa opzione, possono essere utili le routine di riavvio con possibilità di interruzione oppure con funzione di avviso.

Aggiornamento del prodotto con riavvio del sistema necessario dopo l'avvio successivo: l'aggiornamento e il riavvio vengono eseguiti dopo che l'utente ha avviato il computer e si è registrato. Per questa opzione sono consigliabili le routine di riavvio automatiche.

Impostazioni di riavvio

Riavvio del sistema in n secondi

Se l'opzione è attivata, il riavvio necessario viene eseguito **automaticamente** dopo l'esecuzione di un aggiornamento del prodotto secondo l'intervallo di tempo indicato. Compare un conto alla rovescia, senza possibilità di interrompere il riavvio del sistema.

Messaggio di avviso per il riavvio ogni n secondi

Se l'opzione è attivata, il riavvio necessario **non viene eseguito automaticamente** dopo un aggiornamento del prodotto. Nell'intervallo di tempo indicato, vengono visualizzati avvisi di riavvio senza possibilità di interruzione. Negli avvisi è possibile confermare il riavvio del sistema oppure selezionare l'opzione "**Ricorda ancora"**.

Richiesta di esecuzione di riavvio del sistema

Se l'opzione è attivata, il riavvio necessario **non viene eseguito automaticamente** dopo un aggiornamento del prodotto. Viene visualizzato una sola volta un messaggio in cui è possibile confermare il riavvio oppure interrompere la routine di riavvio.

Riavvio del sistema senza richiesta

Se l'opzione è attivata, il riavvio necessario viene eseguito **automaticamente** dopo un aggiornamento del prodotto. Non si riceve alcun messaggio.

L'aggiornamento può essere eseguito mediante server web in Internet .

Connessione al server Web

Utilizza una connessione esistente (rete)

Questa impostazione viene visualizzata se viene utilizzata la connessione mediante una rete.

Utilizzare la seguente connessione:

Questa impostazione viene visualizzata se si definisce individualmente la connessione.

L'Updater riconosce automaticamente quali opzioni di connessione sono disponibili. Le opzioni di connessione non disponibili sono grigie e non possono essere attivate. Ad esempio, è possibile creare manualmente una connessione dial-up mediante una voce dell'elenco telefonico di Windows.

- **Utente:** inserire il nome utente dell'account selezionato.
- **Password:** inserire la password per questo account. Per ragioni di sicurezza i caratteri effettivi che si inseriscono in questo campo vengono visualizzati come asterischi (*).

Suggerimenti
Se sono stati dimenticati il nome utente o la password di un account Internet contattare il provider di servizi Internet.

Suggerimenti
La selezione automatica dell'Updater mediante i cosiddetti strumenti dial-up (ad esempio SmartSurfer, Oleco, ...) attualmente non è ancora disponibile.

Termina la connessione dial-up al termine dell'aggiornamento

Se l'opzione è attivata, viene interrotta automaticamente la connessione dial-up aperta per l'aggiornamento, non appena il download è stato eseguito con successo.

Suggerimenti
L'opzione non è disponibile in Vista. In Vista la connessione dial-up, aperta per l'aggiornamento, viene sempre interrotta, non appena il download è stato eseguito .

13.9 Generale

13.9.1 Categorie di minacce

Selezione categorie delle minacce

Il prodotto AntiVir protegge dai virus del computer.

Inoltre, si ha la possibilità di effettuare una scansione differenziata in base alle seguenti categorie delle minacce.

- Software di gestione backdoor (BDC)
- Programmi di selezione a pagamento (DIALER)
- Giochi (GAMES)
- Programmi ludici (JOKES)
- Security Privacy Risk (SPR)
- Adware/Spyware (ADSPY)
- Programmi zip runtime insoliti (PCK)
- File con estensioni occultate (HEUR-DBLEXT)
- Phishing
- Applicazione (APPL)

Facendo clic sulla casella appropriata viene attivata (spuntata) o disattivata (non spuntata) la modalità selezionata.

Attiva tutti

Se l'opzione è attivata vengono attivate tutte le modalità.

Valori predefiniti

Questo pulsante ripristina i valori standard predefiniti.

Suggerimenti
Se viene disattivata una modalità, i file riconosciuti come tale tipo di programma non verranno più segnalati. Non viene riportata alcuna segnalazione nemmeno sul file di report.

13.9.2 Password

È possibile proteggere il programma AntiVir in diverse sezioni con una password. Se si inserisce una password questa verrà richiesta ogni volta che si desidera aprire una sezione protetta.

Password

Inserimento password

Inserire qui la password desiderata. Per ragioni di sicurezza i caratteri effettivi che si inseriscono in questo campo vengono visualizzati come asterischi (*). È possibile inserire un numero massimo di 20 caratteri. Se è stata inserita una password, il programma negherà l'accesso in caso di inserimento di password errata. Un campo vuoto equivale a "Nessuna password".

Confermare password

Inserire nuovamente la password per conferma. Per ragioni di sicurezza i caratteri effettivi che si inseriscono nel campo vengono visualizzati come asterischi (*).

Suggerimenti
Attenzione alle lettere maiuscole o minuscole!

Aree protette da password

Il programma AntiVir può proteggere singole sezioni con una password. Facendo clic sulla casella appropriata, la richiesta di password per alcune sezioni può essere disattivata o riattivata.

Sezione protetta da password	Funzione
Control Center	Se l'opzione è attivata, per l'avvio del Control Center è necessario inserire la password.
Attiva / Disattiva Guard	Se l'opzione è attivata, per l'attivazione e la disattivazione di AntiVir Guard è necessario inserire la password.
Attiva / disattiva MailGuard	Se l'opzione è attivata, per l'attivazione e la disattivazione del MailGuard è necessario inserire la password.
Attiva/disattiva FireWall	Se l'opzione è attivata, per l'attivazione e la disattivazione del FireWall è necessario inserire la

	password.
Attiva / disattiva WebGuard	Se l'opzione è attivata, per l'attivazione e la disattivazione del WebGuard è necessario inserire la password.
Attiva/Disattiva protezione bambini	Se l'opzione è attivata, per l'attivazione e la disattivazione della protezione bambini è necessario inserire la password.
Quarantena	Se l'opzione è attivata, tutte le sezioni del Gestore della quarantena protette da password sono attivate. Facendo clic sulla casella appropriata, la richiesta di password può essere disattivata o riattivata.
Ripristina gli oggetti infetti	Se l'opzione è attivata, è necessario inserire la password per ripristinare un oggetto.
Nuovo controllo di oggetti infetti	Se l'opzione è attivata, è necessario inserire la password per una verifica successiva.
Apri gli oggetti infetti	Se l'opzione è attivata, è necessario inserire la password per visualizzare le proprietà di un oggetto.
Elimina gli oggetti infetti	Se l'opzione è attivata, è necessario inserire la password per eliminare un oggetto.
Invia email ad Avira	Se l'opzione è attivata, è necessario inserire la password per inviare un oggetto al Malware Research Center Avira per una verifica.
Copia di oggetti infetti	Se l'opzione è attivata, è necessario inserire la password per copiare gli oggetti infetti.
Aggiungi e modifica job	Se l'opzione è attivata, per aggiungere e modificare job nello Scheduler, è necessario inserire la password.
Avvio dell'aggiornamento del prodotto.	Se l'opzione è attivata, all'avvio dell'aggiornamento del prodotto nel menu Aggiorna, è necessario inserire la password.
Configurazione	Se l'opzione è attivata, è possibile configurare il programma solo dopo l'inserimento della password.
Attiva la modalità esperto	Se l'opzione è attivata, per l'attivazione e la disattivazione della modalità esperto, è necessario inserire la password.
Installazione / Disinstallazione	Se l'opzione è attivata, per l'installazione e la disinstallazione del programma, è necessario inserire la password.

13.9.3 Sicurezza

Aggiornamento

Avviso se l'aggiornamento risale a più di n giorni fa

In questo campo, è possibile inserire il numero massimo di giorni che possono trascorrere dall'ultimo aggiornamento. Se si supera questo periodo, il Control Center visualizzerà sotto Stato un'icona rossa per lo stato dell'aggiornamento.

Avvisa se il file VDF non è aggiornato

Se l'opzione è attivata, si riceve un avviso in caso di file di definizione dei virus non aggiornato. Grazie all'opzione Avviso, se l'ultimo aggiornamento risale a più di n giorni, è possibile configurare un intervallo temporale.

Tutela del prodotto

Suggerimenti
Le opzioni per la tutela del prodotto non sono disponibili se il Guard non è stato installato in modo personalizzato.

Proteggi i processi da una chiusura indesiderata

Se l'opzione è attivata, tutti i processi del programma vengono protetti da chiusura indesiderata dovuta a virus e malware o a una chiusura involontaria di un utente, ad esempio mediante il Task Manager. Questa opzione è attivata di default.

Protezione del processo avanzata

Se l'opzione è attivata, tutti i processi del programma vengono protetti da chiusura indesiderata con metodi avanzati. La protezione avanzata del processo consuma molte più risorse rispetto alla protezione di processo base. L'opzione è attivata di default. Per disattivare l'opzione è necessario riavviare il computer.

Importante
Protezione del processo in Windows XP 64 Bit non disponibile!

Attenzione
Se la protezione del processo è attivata, possono verificarsi problemi di interazione con altri software. In tal caso disattivare la protezione del processo.

Proteggi i file e le voci di registrazione dalla manipolazione

Se l'opzione è attivata, tutte le voci del registro del programma e tutti i dati del programma (file binari e di configurazione) vengono protetti da manipolazione. La protezione da manipolazione comprende la protezione da interventi di scrittura, eliminazione e talvolta di lettura sulle voci del registro o sui file di programma da parte di utenti o di programmi estranei. Per attivare l'opzione è necessario riavviare il computer.

Attenzione
Si noti che, se l'opzione è disattivata, la riparazione dei computer colpiti da alcuni tipi di malware può fallire.

Suggerimenti
Se l'opzione è attivata, è possibile effettuare modifiche della configurazione o di job di scansione e aggiornamento solo tramite l'interfaccia utente.

Importante
Protezione dei file e delle voci di registrazione in Windows XP 64 Bit non disponibile!

13.9.4 WMI

Supporto per Windows Management Instrumentation

Windows Management Instrumentation è una tecnologia di gestione fondamentale di Windows che consente, mediante linguaggi di script e di programmazione in lettura e in scrittura, di accedere in locale e in remoto alle impostazioni dei computer Windows. Il programma AntiVir supporta WMI e rende disponibili Dati (informazioni sullo stato, statistiche, rapporti, job pianificati ecc.), eventi tramite un'interfaccia. Tramite WMI è possibile richiamare dati operativi del programma.

attiva supporto WMI

Se l'opzione è attivata, è possibile richiamare i dati operativi del programma tramite WMI.

13.9.5 Directory

Percorso temporaneo

In questo campo inserire il percorso in cui i file temporanei del programma dovranno essere salvati.

Utilizza le impostazioni predefinite

Se l'opzione è attivata vengono utilizzate le impostazioni del sistema per la gestione dei file temporanei.

Suggerimenti
I file temporanei nel sistema sono memorizzati ad esempio in Windows XP - in: Start | Impostazioni | Pannello di controllo | Sistema | Scheda "Avanzate" | Pulsanti "Variabili d'ambiente". Le variabili temporanee (TEMP, TMP) per l'utente di volta in volta registrato e per le variabili di sistema (TEMP, TMP) sono visibili qui con i loro rispettivi valori.

Utilizzare la seguente directory

Se l'opzione è attivata viene utilizzato il percorso visualizzato nel campo.

Il pulsante apre una finestra nella quale si ha la possibilità di selezionare il percorso temporaneo desiderato.

Standard

Il pulsante crea la directory predefinita per il percorso temporaneo.

13.9.6 Proxy

Proxyserver

Non utilizzare un server Proxy

Se l'opzione è attivata, la connessione al server web viene effettuata mediante un server proxy.

Utilizza impostazioni di sistema di Windows

Se l'opzione è attivata, vengono utilizzate le impostazioni di sistema di Windows correnti per la connessione al server Web mediante un server proxy. È possibile configurare le impostazioni di sistema di Windows per l'utilizzo di un server proxy nel **Pannello di controllo:: Opzioni internet :: Connessioni :: Impostazioni LAN**. È possibile accedere alle opzioni internet anche nel menu Extra di Internet Explorer.

Attenzione
Quando si utilizza un server proxy che richiede l'autenticazione, immettere tutti i dati tramite l'opzione *Utilizza questo server proxy*. Per i server proxy senza autenticazione, è possibile utilizzare l'opzione *Utilizza impostazioni di sistema di Windows*.

Utilizza questo server proxy

Se l'opzione è attivata, la connessione al server web avviene mediante un server proxy, utilizzando le impostazioni definite.

Indirizzo

Immettere il nome computer o l'indirizzo IP del server proxy che si desidera utilizzare per la connessione al server Web.

Porta

Immettere il numero della porta del server proxy che si desidera utilizzare per la connessione al server Web.

Nome Login

Immettere un nome utente per la registrazione sul server proxy.

Password

Inserire la password appropriata per la registrazione sul server proxy. Per ragioni di sicurezza i caratteri effettivi che si inseriscono nel campo vengono visualizzati come asterischi (*).

Esempi:

Indirizzo:	proxy.domain.de	Porta:	8080
Indirizzo:	192.168.1.100	Porta:	3128

13.9.7 Eventi

Limitare l'estensione della banca dati degli eventi

Limita l'estensione ad un massimo di n immissioni

Se l'opzione è attiva, il numero massimo delle immissioni nella banca dati degli eventi è limitato a un preciso numero; i valori consentiti sono: da 100 a 10.000 immissioni. Se il numero delle immissioni viene superato gli inserimenti più vecchi vengono eliminati.

Elimina tutti gli eventi più vecchi di n giorno/i

Se l'opzione è attiva dopo un numero determinato di giorni gli eventi vengono eliminati dalla banca dati degli eventi; i valori consentiti sono: da 1 a 90 giorni. Di default questa opzione è attivata con un valore di 30 giorni.

Non limitare estensione banca dati (elimina eventi manualmente)

Con l'opzione attivata, le dimensioni della banca dati degli eventi non sono limitate. Sull'interfaccia del programma, alla voce Eventi, viene però visualizzato un massimo di 20.000 immissioni.

13.9.8 Limita i report

Limita il numero di report

Limita il numero a n pezzi

Se l'opzione è attiva, il numero massimo di report può essere limitato; i valori consentiti sono: da 1 a 300. Se il numero indicato viene superato, i report più vecchi vengono eliminati.

Elimina tutti i report più vecchi di n giorni

Se l'opzione è attiva i report vengono automaticamente eliminati dopo un determinato numero di giorni; i valori consentiti sono: da 1 a 90 giorni. Di default questa opzione è attivata con un valore di 30 giorni.

Non limitare il numero dei report (elimina manualmente i report)

Se l'opzione è attiva, il numero di report non è limitato.

13.9.9 Avvisi acustici

Avviso acustico

In caso di rilevamento di un virus o di un malware tramite sistema di scansione o Guard viene emesso un avviso acustico in modalità di azione interattiva. È possibile attivare o disattivare l'avviso acustico oppure selezionare un file wave alternativo come avviso acustico.

Suggerimenti
La modalità di azione del sistema di scansione viene impostata nella configurazione in Sistema di scansione::Scansione::Azione in caso di rilevamento. La modalità di azione del Guard viene impostata nella configurazione in Guard::Scansione::Azione in caso di rilevamento.

Nessun avviso

Se l'opzione è attivata, non viene emesso alcun avviso acustico in caso di rilevamento tramite il sistema di scansione o il Guard.

Emetti tramite casse PC (solo in modalità interattiva)

Se l'opzione è attivata, viene emesso un avviso acustico con suono standard in caso di rilevamento di un virus tramite sistema di scansione o Guard. L'avviso acustico viene emesso tramite l'altoparlante interno del PC.

Utilizza il seguente file wave (solo in modalità interattiva)

Se l'opzione è attivata, in caso di rilevamento di un virus tramite sistema di scansione o Guard viene emesso un avviso acustico con il file wave selezionato. Il file wave selezionato viene riprodotto tramite un altoparlante collegato esternamente.

File audio (.WAV)

In questo campo è possibile inserire il nome e il percorso corrispondente di un file audio. L'avviso acustico standard del programma viene immesso di default.

Il pulsante apre una finestra nella quale si ha la possibilità di selezionare il file desiderato grazie all'explorer dei file.

Test

Questo pulsante serve a testare il file wave selezionato.

13.9.10 Avvisi

Il programma AntiVir, in caso di determinati eventi, genera un messaggi sul desktop, i cosiddetti messaggi a tendina, per informare l'utente di eventuali pericoli o della riuscita o meno dell'esecuzione di un dato programma come, per esempio, un aggiornamento. È possibile attivare o disattivare in *Avvisi* la funzione di notifica per specifici eventi.

Nel caso delle notifiche sul desktop è possibile disattivare direttamente le notifiche sul messaggio a tendina. È possibile annullare la disattivazione della notifica in *Avvisi*.

Avvisi

sulle connessioni dial-up utilizzate

Se l'opzione è attivata, l'utente è avvisato con una notifica sul desktop quando un programma di selezione stabilisce una connessione sul computer tramite la rete telefonica o ISDN. In caso di programmi di selezione esiste il rischio che si tratti di un dialer sconosciuto e indesiderato, che stabilisce una connessione a pagamento. (vedere Virus e altro::Categorie delle minacce: Dialer).

sul corretto aggiornamento dei file

Se l'opzione è attivata, l'utente riceve un messaggio sul desktop quando è stato completato con successo un aggiornamento e sono stati aggiornati file.

su aggiornamento fallito

Se l'opzione è attivata, l'utente riceve un messaggio sul desktop quando un aggiornamento non è stato completato con successo: Non è stato possibile stabilire una connessione con il server di download o non è stato possibile installare i file aggiornati.

non è necessario alcun aggiornamento

Se l'opzione è attivata, l'utente riceve un messaggio sul desktop quando è stato lanciato un aggiornamento ma non era necessario installare alcun file perché il programma era già aggiornato.